Algebra superiore 1
Prof. Giovanni Gaiffi

Stefano Maggiolo
http://poisson.phc.unipi.it/~maggiolo/
maggiolo@mail.dm.unipi.it

2006–2007

Indice

1 Gruppi di Lie **3**
1.1 Introduzione 3
1.2 Sottogruppi di Lie 6
1.3 Teoria delle rappresentazioni dei gruppi topologici 10
1.4 Tori 11

2 Algebre di Lie **14**
2.1 Introduzione 14
2.2 Algebre di Lie semisemplici 17
2.3 Teoria delle rappresentazioni delle algebre di Lie 21
2.4 Algebre risolubili, radicale e teorema di Lie 24
2.5 Il sistema di radici 25
2.6 Teorema di Poincaré-Birkhoff-Witt 28
2.7 Teoria delle rappresentazioni delle algebre di Lie semisemplici complesse 33

3 Risultati ulteriori **37**
3.1 Decomposizione di Levi 37
3.2 Teorema di Ado 38

4 Complementi **39**
4.1 Sistemi di radici 39
4.2 Gruppi topologici 46
4.3 Algebre di Clifford 51

1 Gruppi di Lie

01.03.2007

1.1 Introduzione

Definizione 1.1.1. Un *gruppo di Lie* è:

1. una varietà[1] C^∞, M;
2. una struttura di gruppo su M data da una moltiplicazione μ e da una inversa i;
3. una compatibilità tra i primi due punti: μ e i sono C^∞.

Definizione 1.1.2. Un *morfismo* ϑ tra i gruppi di Lie G e H è:

1. un morfismo di gruppi;
2. una mappa C^∞.

Teorema 1.1.3. *Sia $\varphi\colon G \to H$ un morfismo di gruppi tra due gruppi di Lie; se φ è continuo, allora $\varphi \in \mathrm{C}^\infty$.*

Dato un gruppo di Lie G, si vuole studiare il piano tangente nell'identità, chiamato $G_e := \mathrm{T}\, G_e$. Si studieranno inizialmente tutti i morfismi di gruppi di Lie $\mathbb{R} \to G$, dove $\mathbb{R}$ ha la struttura di gruppo di Lie data dalla somma. Questi morfismi saranno dei cammini C^∞ dentro G, caratterizzati dal fatto che il tangente del cammino nell'identità determina univocamente il cammino: si mostrerà che il tangente è in corrispondenza biunivoca con i morfismi da $\mathbb{R}$ in G. Questo servirà per definire una mappa ("esponenziale") $G_e \to G$ che sarà la parametrizzazione principale per studiare il gruppo.

Definizione 1.1.4. Un *sottogruppo a un parametro* di un gruppo di Lie G è un morfismo di gruppi di Lie da $\mathbb{R}$ a G.

Il piano $\mathbb{R}^2$ è un gruppo di Lie, così come ${}^{\mathbb{R}^2}\!/\!{}_{\mathbb{Z}^2}$; se si considera $\vartheta\colon \mathbb{R} \to \mathbb{R}^2$ con $\vartheta(s) = (s, cs)$, con $c \in \mathbb{R}$, questo è un morfismo di gruppi di Lie che può essere proiettato al quoziente.

Definizione 1.1.5. Sia G un gruppo di Lie; per ogni $g \in G$, sia $L_g\colon G \to G$ la mappa definita da $L_g(x) := gx$. Un campo di vettori λ si dice *invariante a sinistra*[2] se per ogni $x \in G$, $\lambda \circ L_g(x) = L'_g \circ \lambda(x)$.

Teorema 1.1.6. *C'è una corrispondenza biunivoca tra i sottogruppi a un parametro di G e gli elementi di G_e, tramite la mappa $\vartheta \mapsto \vartheta'(u_0)$, dove u_0 è il vettore unitario in $\mathbb{R}_0$ e ϑ' è visto come differenziale.*

[1] A volte si richiede che la varietà sia analitica; tuttavia se anche si richiedesse che tutto fosse C^0, esiste un'unica struttura analitica compatibile con la struttura C^0 che rende la varietà un gruppo di Lie analitico. Sapere se si può mettere su un gruppo di Lie C^0 una struttura di gruppo di Lie analitico è il quinto problema di Hilbert, risolto da Von Neumann nel 1933 per i gruppi compatti e poi da Gleason, Montgomery e Zippin nel caso generale.

[2] Dalla definizione si ha che se un campo di vettori invariante a sinistra è noto in un punto, allora è noto ovunque.

Dimostrazione. **Unicità.** Siano ϑ un sottogruppo a un parametro, $v := \vartheta'(u_0)$: il diagramma

$$\begin{tikzcd} \mathbb{R} \arrow[r, "\vartheta"] \arrow[d, "L_s"'] & G \arrow[d, "L_{\vartheta(s)}"] \\ \mathbb{R} \arrow[r, "\vartheta"'] & G \end{tikzcd}$$

commuta, poiché ϑ è un morfismo. Sia u_s il campo di vettori invariante a sinistra su $\mathbb{R}$ ottenuto da u_0 mediante la traslazione; sia v_x il campo di vettori invariante a sinistra su G tale che $v_e = v$. Allora dal diagramma commutativo, per ogni $\tilde{u} \in \mathrm{T}\,\mathbb{R}_s$, si ha $\vartheta' \circ L'_s(\tilde{u}) = L'_{\vartheta(s)} \circ \vartheta'(\tilde{u})$, e in particolare vale in u_0, cioè $\vartheta'(u_s) = v_{\vartheta(s)}$. Considerando questa equazione e la condizione iniziale $\vartheta'(u_0) = v$, si ha un'equazione differenziale che deve essere soddisfatta da qualsiasi sottogruppo a un parametro, da cui segue l'unicità.

Esistenza. Siano $v \in G_e$, v_x come prima il campo di vettori invariante a sinistra tale che $v_e = v$. Si cerca ϑ tale che $\vartheta'(u_s) = v_{\vartheta(s)}$ e $\vartheta'(u_0) = v$. Chiaramente $\vartheta(0) = e$. Per il teorema di esistenza locale, tale ϑ si trova, localmente: $\vartheta\colon (-\varepsilon, \varepsilon) \to G$. Tuttavia, già ora $\vartheta(s + t) = \vartheta(s)\vartheta(t)$, perché entrambe, fissato s e lasciando variare t, soddisfano l'equazione differenziale, anche se con condizione iniziale $\vartheta'(u_0) = v_{\vartheta(s)}$: infatti, derivando rispetto a t e valutando in 0 si ottiene da una parte $\vartheta'(u_s) = \vartheta' \circ L'_s(u_0)$ e dall'altra $L'_{\vartheta(s)} \circ \vartheta'(u_0)$, che coincidono per la commutatività del diagramma precedente ed equivalgono a $v_{\vartheta(s)}$.

Per estendere ϑ, si potrebbe considerare $\tilde{\vartheta}(s) := \vartheta({}^{s}\!/_{M})^M$, con M tale che ${}^{s}\!/_{M} \in (-\varepsilon, \varepsilon)$. Bisogna verificare che sia ben definito, che sia un morfismo e che sia differenziabile:

- è ben definito perché $\vartheta({}^{s}\!/_{N})^N = \vartheta({}^{s}\!/_{MN})^{MN}$, dato che l'immagine di $\mathbb{R}$ commuta;
- è un morfismo perché, posto N abbastanza grande, $\tilde{\vartheta}(t + s) = \vartheta({}^{s}\!/_{N} + {}^{t}\!/_{N})^N = (\vartheta({}^{s}\!/_{N})\vartheta({}^{t}\!/_{N}))^N$; l'elevamento alla N non crea problemi perché essendo ϑ un morfismo, i valori $\vartheta({}^{s}\!/_{N})$ e $\vartheta({}^{t}\!/_{N})$ commutano;
- per esercizio. □

Definizione 1.1.7. Si definisce la *mappa esponenziale* $\exp\colon G_e \to G$: dato $v \in G_e$, sia ϑ_v il sottogruppo a un parametro associato a v; si pone $\exp(v) := \vartheta_v(1)$. In particolare, $\exp(sv) = \vartheta_v(s)$.

Esempio 1.1.8. Sia V uno spazio vettoriale; allora $\mathrm{Aut}(V)$ è un gruppo di Lie: fissata una base, la moltiplicazione per matrici è chiaramente C^∞; l'inversa ha solo il determinante al denominatore, ma in $\mathrm{Aut}(V)$ il determinante è mai nullo. Il gruppo degli automorfismi può essere visto come un aperto di $\mathrm{End}(V)$, quindi $\mathrm{Aut}(V)_e$ può essere identificato con $\mathrm{End}(V)$. Sia $A \in \mathrm{End}(V)$; allora la mappa esponenziale dovrebbe restituire una matrice in $\mathrm{Aut}(V)$: infatti si verifica che $sA \mapsto \mathrm{Id} + sA + {}^{1}\!/_{2}s^2A^2 + \cdots =: e^{sA}$ è la mappa esponenziale.

Teorema 1.1.9. *La mappa esponenziale è* C^∞.

Dimostrazione. Segue da $\vartheta_v'(u_s) = v_{\vartheta_v(s)} = L'_{\vartheta_v(s)}(v)$, grazie al teorema per cui la soluzione dell'equazione differenziale dipende in modo C^∞ da v e da s. $\square$

Teorema 1.1.10. *Dato un morfismo di gruppi di Lie $\varphi\colon G \to H$, il diagramma*

$$\begin{tikzcd} G_e \arrow[r, "\varphi'"] \arrow[d, "\exp"'] & H_e \arrow[d, "\exp"] \\ G \arrow[r, "\varphi"'] & H \end{tikzcd}$$

commuta[3].

Dimostrazione. Fissato $v \in G_e$, $\varphi \circ \vartheta_v$ è un sottogruppo a un parametro di H, quello che nel tangente all'identità ha $\varphi'(v)$; ma anche $\vartheta_{\varphi'(v)}$ soddisfa la stessa condizione, quindi coincidono. $\square$

Teorema 1.1.11. *La mappa esponenziale è un diffeomorfismo da un intorno di $0 \in G_e$ a un intorno di $e \in G$ (è un diffeomorfismo locale).*

Dimostrazione. Si considera il differenziale dell'esponenziale applicato a $v \in G_e$, identificando $\mathrm{T}(G_e)$ con G_e:

$$\exp'(v) = \left[\frac{\mathrm{d}}{\mathrm{d}s}\exp(sv)\right]_{s=0} = \left[\frac{\mathrm{d}}{\mathrm{d}s}\vartheta_v(s)\right]_{s=0} = v;$$

allora il differenziale dell'esponenziale nell'identità si identifica con l'identità, quindi localmente exp è un diffeomorfismo. $\square$

Osservazione 1.1.12. Se G_1 è la componente connessa di G che contiene l'identità, G_1 è un sottogruppo di G? Se $g_1 \in G_1$, $g_1 G_1 = L_{g_1}(G_1)$ è l'immagine del connesso G_1 tramite la mappa continua L_{g_1}, quindi è connesso e contiene g_1 (perché $e \in G_1$); quindi G_1 è chiuso per moltiplicazione. Inoltre $i(G_1)$ è un connesso che contiene l'identità, perciò G_1 è un sottogruppo. Al tangente nell'identità quindi sfuggiranno le proprietà delle altre componenti connesse.

Proposizione 1.1.13. *Sia $S \subseteq G_1$ un intorno di e; allora il sottogruppo generato da S è G_1.*

Dimostrazione. Il sottogruppo generato da S è aperto: se $s \in \langle S\rangle$, anche $sS \subseteq \langle S\rangle$ e sS è un intorno di s. Ma è anche chiuso: se $g \notin \langle S\rangle$, allora anche $gS \cap \langle S\rangle = \varnothing$, altrimenti esisterebbe $x \in gS \cap \langle S\rangle$, cioè $x = gs \in \langle S\rangle$ e si avrebbe $g = xs^{-1} \in \langle S\rangle$, assurdo. $\square$

Teorema 1.1.14. *Se G è connesso, un morfismo di gruppi di Lie $\vartheta\colon G \to H$ è completamente determinato da $\vartheta'_{|G_e}\colon G_e \to H_e$.*

Dimostrazione. Segue dalla proposizione 1.1.13 insieme al teorema 1.1.10. $\square$

06.03.2007

Lemma 1.1.15. *Sia $\varphi\colon U \to G$ una carta che manda $0 \in U$ in $e \in G$. Presi $x, y \in U$ sufficientemente piccoli (in modo che $\varphi(x)\varphi(y) \in \varphi(U)$), si può scrivere la moltiplicazione di x e y come $\varphi^{-1}(\varphi(x)\varphi(y)) = \mu(x,y) = x + y + \mathrm{o}(r)$, dove r è la distanza di (x,y) da $(0,0)$ dopo aver scelto una metrica su U.*

[3]Quindi, conoscendo φ' si conosce φ. Questo è importante perché sui tangenti all'identità si riuscirà a mettere una struttura di algebra; perciò le mappe tra gruppi di Lie si trasformano in mappe tra algebre di Lie.

Dimostrazione. Si può scrivere $\mu(x, y) = a + Cx + By + \mathrm{o}(r)$, sviluppando al primo ordine. Per $x = 0$, $y = \mu(0, y) = a + By + \mathrm{o}(r)$: al variare di y, si ottiene che $B = I$ e $a = 0$ e allo stesso modo si ottiene che anche $C = I$. □

Teorema 1.1.16. *Un gruppo di Lie abeliano connesso è della forma $T^a \times \mathbb{R}^b$, dove T è S^1.*

Dimostrazione. Nel caso abeliano, exp è un morfismo $G_e \to G$, infatti dalla definizione di exp, dalla abelianità e dal lemma 1.1.15 (considerando exp come una carta), si ha:

$$\begin{aligned}\exp(V)\exp(W) &= \exp\left(\frac{V}{N}\right)^N \exp\left(\frac{W}{N}\right)^N = \left(\exp\left(\frac{V}{N}\right)\exp\left(\frac{W}{N}\right)\right)^N = \\ &= \exp\left(\frac{V}{N} + \frac{W}{N} + \mathrm{o}\left(\frac{1}{N}\right)\right)^N = \exp\left(\frac{V + W + \mathrm{o}(1)}{N}\right)^N = \\ &= \exp(V + W + \mathrm{o}(1)) \xrightarrow{N \to +\infty} \exp(V + W).\end{aligned}$$

Allora $\exp(G_e)$ genera tutto G poiché G è connesso e exp è un diffeomorfismo in un intorno dell'identità, ma essendo $\exp(G_e)$ un sottogruppo, $\exp(G_e) = \langle \exp(G_e) \rangle = G$. In questo particolare caso, l'esponenziale è un morfismo suriettivo ed è un diffeomorfismo attorno all'identità. Questo implica che il suo nucleo è discreto e $G = {}^{G_e}/_{\ker \exp}$. Ora, i sottogruppi discreti di $\mathbb{R}^n$ sono gruppi abeliani liberi generati da $g_1, \ldots, g_r$ linearmente indipendenti su $\mathbb{R}$ e con $r \leq n$. Si considera quindi la base di G_e data da $g_1, \ldots, g_r, h_{r+1}, \ldots, h_n$; in questa base, $\ker \exp = \mathbb{Z}^r \times \{0\}^{n-r}$, e $G = {}^{\mathbb{R}^n}/_{\ker \exp} = T^r \times \mathbb{R}^{n-r}$. □

Esercizio 1.1.17. Trovare i gruppi di Lie abeliani compatti.

1.2 Sottogruppi di Lie

Definizione 1.2.1. Un *sottogruppo di Lie* di un gruppo di Lie G è dato da un morfismo iniettivo di gruppi di Lie $f\colon H \to G$.

Definizione 1.2.2. Sia $\gamma\colon N \to M$; se il differenziale di γ è iniettivo, N si dice *immersed*; se inoltre γ è iniettiva, N si dice *imbedded*; se γ è anche un omeomorfismo con l'immagine, N si dice *embedded* o *regolare*. In quest'ultimo caso le strutture topologiche dell'immagine come sottospazio di M e come immagine di γ coincidono.

Osservazione 1.2.3. Se $f\colon H \to G$ è un morfismo di gruppi di Lie iniettivo, allora è sempre un imbedding. Infatti $f'_{|H_e}$ è iniettivo: se $v \in H_e$ è tale che $f'(v) = 0$, per la linearità si può assumere che v appartenga a un intorno dell'identità sul quale exp è un diffeomorfismo, allora $e = \exp(f'(v)) = f(\exp(v))$ e ciò implica $\exp(v) = e$, cioè $v = 0$. D'altra parte, $f'(L'_g(x)) = L'_{f(g)}f'(x)$, cioè anche $f'_{\mathrm{T}\,G_g}$ è iniettivo, dal fatto che L'_g è un diffeomorfismo globale.

Esempio 1.2.4. Sia $\mathbb{Z} \to S^1$ la mappa che manda n in e^{in}: è un morfismo di gruppi di Lie iniettivo, quindi è un imbedding, ma non è un embedding, poiché la sua immagine è densa e la topologia dell'immagine non può essere discreta come quella di $\mathbb{Z}$.

Definizione 1.2.5. Sia $\pi\colon N \to M$ un imbedding; π è *quasi regolare* se per ogni $f\colon X \to N$, $f \in \mathrm{C}^\infty$ se e solo se $\pi \circ f \in \mathrm{C}^\infty$.

Esempio 1.2.6. La mappa

$$\begin{array}{rccl} f\colon & \mathbb{R} & \longrightarrow & T^2 \\ & t & \longmapsto & (e^{2\pi i t}, e^{2\pi i \alpha t}), \end{array}$$

con $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, è quasi regolare ma non è un embedding.

Teorema 1.2.7. *Un sottogruppo astratto H di un gruppo di Lie G è una sottovarietà regolare se e solo se H è chiuso.*

Dimostrazione. $\Rightarrow$ Se H è un embedding in G, esiste un intorno U di $e \in G$ tale che $H \cap U$ è un insieme coordinato, in particolare $H \cap U$ è chiuso in U. Sia $y \in \bar{H}$; yU^{-1} è un intorno di y, allora esiste $x \in yU^{-1} \cap H$; in particolare $x \in H$ e $y \in \bar{H} \cap xU$; allora $x^{-1}y \in \bar{H} \cap U = H \cap U$, perché $H \cap U$ è chiuso in U. Infine $x^{-1}y \in H$ implica $y \in H$.

$\Leftarrow$ Verrà dimostrata in seguito. □

Esempio 1.2.8. Si considera

$$\mathrm{O}(n, \mathbb{R}) \coloneqq \left\{ A \in \mathrm{GL}(n, \mathbb{R}) \mid AA^t = A^tA = I \right\} \subseteq \mathrm{GL}(n, \mathbb{R}):$$

questo è un sottogruppo chiuso perché dato da una condizione chiusa, quindi è un sottogruppo di Lie; anche

$$\mathrm{U}(n) \coloneqq \left\{ A \in \mathrm{GL}(n, \mathbb{C}) \mid A\bar{A}^t = \bar{A}^tA = I \right\} \subseteq \mathrm{GL}(n, \mathbb{C})$$

è un sottogruppo di Lie, per lo stesso motivo. Tuttavia, $\mathrm{U}(n)$ è un sottogruppo di Lie di $\mathrm{GL}(n, \mathbb{C})$ visto come gruppo di Lie reale, ma non è un sottogruppo di Lie complesso, perché la mappa che dà l'inverso è $A \mapsto \bar{A}^t$, che non è una trasformazione olomorfa.

Si era visto che era possibile identificare $\mathrm{GL}(n, \mathbb{R})_e$ con $\mathrm{End}(\mathbb{R}^n) =: \mathfrak{gl}(n, \mathbb{R})$ e che l'esponenziale è l'esponenziale matriciale. Nel caso di sottogruppi di Lie, l'esponenziale è la restrizione dell'esponenziale al sottogruppo, e si possono vedere le seguenti:

$$\begin{aligned} \mathrm{O}(n, \mathbb{R})_e &= \left\{ A \in \mathrm{End}(\mathbb{R}^n) \mid A + A^t = 0 \right\}, \\ \mathrm{U}(n)_e &= \left\{ A \in \mathrm{End}(\mathbb{C}^n) \mid A + \bar{A}^t = 0 \right\}. \end{aligned}$$

Infatti, se f è un sottogruppo a un parametro contenuto in $\mathrm{O}(n, \mathbb{R})$ con $f'(u_0) = A$, allora si può scrivere come $f(s) = I + As + \mathrm{o}(s) \in \mathrm{O}(n, \mathbb{R})$ e si ottiene

$$I = f(s)f(s)^t = (I + As + \mathrm{o}(s))(I + A^ts + \mathrm{o}(s)) = I + (A + A^t)s + \mathrm{o}(s),$$

da cui $A + A^t = 0$. Viceversa, se $A + A^t = 0$, basta verificare che $\exp(A) \in \mathrm{O}(n, \mathbb{R})$, ma $A^t = -A$, perciò A e A^t commutano e

$$\exp(A)\exp(A)^t = e^A(e^A)^t = e^Ae^{A^t} = e^{A+A^t} = e^0 = I.$$

Per $\mathrm{U}(n)$ si procede esattamente allo stesso modo.

13.03.2007

Esempio 1.2.9. Si definisce il *corpo dei quaternioni* come

$$\mathbb{H} := \{\, a + bi + cj + dk \mid a, b, c, d \in \mathbb{R} \,\},$$

con le relazioni

$$\begin{array}{lll} i^2 = -1 & j^2 = -1 & k^2 = -1 \\ ij = k & jk = i & ki = j \\ ji = -k & kj = -i & ik = -j. \end{array}$$

Con questa moltiplicazione, $\mathbb{H}$ è un corpo non commutativo. I quaternioni si possono anche rappresentare come matrici in $\mathscr{M}_2(\mathbb{C})$ della forma $\left(\begin{smallmatrix} a & b \\ -\bar{b} & \bar{a} \end{smallmatrix}\right)$, dove gli elementi speciali sono $1 = I$, $i = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$, $j = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, $k = \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right)$. Se $h = a + bi + cj + dk$, $\bar{h} := a - bi - cj - dk$ e si può definire la norma di h come $|h| := h\bar{h}$, che si dimostra essere il determinante della matrice che rappresenta h. Nella rappresentazione matriciale, si vede che gli elementi di norma 1 sono quelli per cui $|a|^2 + |b|^2 = 1$, cioè $\{\, h \in \mathbb{H} \mid |h| = 1 \,\} = \mathrm{SU}(2)$.

Il calcolo precedente vale anche se si considerano i quaternioni e

$$\mathrm{Sp}(n) := \left\{\, A \in \mathrm{GL}(n, \mathbb{H}) \mid \bar{A}^t A = A\bar{A}^t = I \,\right\},$$

il gruppo delle trasformazioni unitarie quaternioniche, tenendo presente che la moltiplicazione nei quaternioni non è commutativa: se $\varphi = (\varphi_{\lambda,\nu})$ e $\psi = (\psi_{\mu,\lambda})$ sono elementi di $\mathrm{GL}(n, \mathbb{H})$, allora la composizione è data da $(\psi\varphi)_{\mu,\nu} = \sum_\lambda \varphi_{\lambda,\nu}\psi_{\mu,\lambda}$.

Se V è uno spazio vettoriale su $\mathbb{H}$, si può estendere la norma hermitiana a V: se $v = \sum a_i v_i$ e $w = \sum b_i w_i \in V$, si definisce $\langle v, w\rangle := \sum a_i \bar{b_i}$; questo è un prodotto scalare e si prende la norma corrispondente. Ora, avendo la norma, si ha $\mathrm{Sp}(n) := \{\, \varphi \in \mathrm{GL}(n, \mathbb{H}) \mid (\forall v \in V)\, |v| = |\varphi(v)| \,\}$.

Si può dimostrare che $\mathrm{Sp}(n) = \mathrm{Sp}(2n, \mathbb{C}) \cap \mathrm{U}(2n)$, dove, posto $J := \left(\begin{smallmatrix} 0 & -I \\ I & 0 \end{smallmatrix}\right)$, $\mathrm{Sp}(2n, \mathbb{C}) = \{\, A \in \mathrm{GL}(2n, \mathbb{C}) \mid A^t J A = J \,\}$. Anche questo è un gruppo di Lie, inoltre è un sottogruppo astratto e chiuso di $\mathrm{GL}(2n, \mathbb{C})$, quindi è un sottogruppo di Lie. Per scoprire com'è fatto il tangente a $\mathrm{Sp}(2n, \mathbb{C})$, si considerano i sottogruppi a un parametro: gli elementi X di $\mathfrak{sp}(2n, \mathbb{C})$ soddisfano $(e^{sX})^t J e^{sX} = J$; questa relazione si può vedere come un'uguaglianza tra i due sottogruppi a un parametro Je^{sX} e $(e^{-sX})^t J$; di conseguenza, derivando e valutando in 0, si ha l'uguaglianza $JX = -X^t J$, perciò il tangente è $\left\{\, X \in \mathfrak{gl}(\mathbb{C}^{2n}) \mid JX = -X^t J \,\right\}$ (l'inclusione inversa è ovvia)[4].

Ora, si vede $\mathbb{H}^n$ come $\mathbb{C}^n \oplus \mathbb{C}^n j$; una mappa $\varphi\colon \mathbb{C}^n \oplus \mathbb{C}^n j \to \mathbb{C}^n \oplus \mathbb{C}^n j$ è $\mathbb{H}$-lineare se e solo se commuta con la mappa $\mathbb{R}$-lineare definita dalla moltiplicazione a sinistra per j, cioè $u + vj \mapsto -\bar{v} + \bar{u}j$. Inoltre la norma di $\mathbb{H}^n$ è la stessa norma indotta da $\mathbb{C}^n \oplus \mathbb{C}^n j$, quindi $\mathrm{Sp}(n) \subseteq \mathrm{U}(2n)$; ma vale anche $\mathrm{Sp}(n) \subseteq \mathrm{Sp}(2n, \mathbb{C})$ con una verifica diretta.

Si è completata una inclusione: per dire che sono uguali, grazie al diffeomorfismo dato dalla mappa esponenziale, si può dire che i tangenti hanno la stessa

[4] In generale, se si ha un gruppo che rispetta la forma bilineare f, cioè tale che per ogni $g \in G$, $f(v, w) = f(gv, gw)$, allora nel tangente si avranno gli elementi X tali che $f(Xv, w) + f(v, Xw) = 0$.

dimensione su $\mathbb{R}$, dacché ovviamente il tangente di $\mathrm{Sp}(n)$ è contenuto nell'intersezione dei tangenti di $\mathrm{Sp}(n)$ e $\mathrm{U}(2n)$. I tangenti di $\mathrm{Sp}(n)$, $\mathrm{U}(2n)$ e $\mathrm{Sp}(2n,\mathbb{C})$ sono rispettivamente

$$\begin{aligned}
\mathfrak{sp}(n) &= \left\{ X \in \mathfrak{gl}(\mathbb{H}^n) \mid \bar{X}^t = -X \right\} \text{ (con il coniugato quaternionico)},\\
\mathfrak{u}(2n) &= \left\{ X \in \mathfrak{gl}(\mathbb{C}^{2n}) \mid \bar{X}^t = -X \right\} \text{ (con il coniugato complesso)},\\
\mathfrak{sp}(2n,\mathbb{C}) &= \left\{ X \in \mathfrak{gl}(\mathbb{C}^{2n}) \mid JX = -X^t J \right\}.
\end{aligned}$$

A questo punto si calcolano le dimensioni e si osserva che sono entrambe uguali a $2n^2+n$.

Ora, questi due gruppi avendo lo stesso tangente, hanno un intorno dell'identità isomorfo, che si è visto generare la componente connessa a cui appartiene l'identità; si deve mostrare che sono connessi. Per fare questo si studia il quoziente ${}^{\mathrm{Sp}(n)}/_{\mathrm{Sp}(n-1)}$, dove $\mathrm{Sp}(n-1)$ si vede come $\{ \varphi \in \mathrm{Sp}(n) \mid \varphi(v_1) = v_1 \}$. Sia $S(\mathbb{H}^n) := S^{4n-1}$ la sfera unitaria dentro $\mathbb{H}^n$, allora si definisce la mappa $\mathrm{Sp}(n) \to S(\mathbb{H}^n)\colon \varphi \mapsto \varphi(v_1)$: è una mappa suriettiva e il suo nucleo è $\mathrm{Sp}(n-1)$, da cui si ha che ${}^{\mathrm{Sp}(n)}/_{\mathrm{Sp}(n-1)}$ è omeomorfo a S^{4n-1}: la mappa è continua e invertibile e la compattezza della sfera dà la continuità dell'inversa. Infine, per induzione, $\mathrm{Sp}(1) = \mathrm{SU}(2) = S^3$ è connesso; se $\mathrm{Sp}(n-1)$ è connesso, si suppone per assurdo che $\mathrm{Sp}(n)$ sia unione disgiunta di chiusi; allora la fibra di $\varphi(v_1)$ è $\mathrm{Sp}(n-1)$, quindi è connessa e sarebbe contenuta tutta in uno di questi chiusi, che di conseguenza sarebbero saturi e si potrebbero trasportare su S^{4n-1}, assurdo.

Esempio 1.2.10. Si considera $\mathrm{SL}(n,\mathbb{C}) = \{ A \in \mathrm{GL}(n,\mathbb{C}) \mid \det A = 1 \}$. Il suo tangente nell'identità è $\{ X \in \mathrm{End}(\mathbb{C}^n) \mid \operatorname{Tr} X = 0 \}$: se X ha traccia 0, su una base che la triangola e^{sX} ha sulla diagonale $e^{s\lambda_i}$, dove λ_i sono gli autovalori; di conseguenza $\det e^{sX} = 1$. D'altra parte, le dimensioni corrispondono, quindi quello è tutto il tangente.

Ora si concluderà la dimostrazione del teorema 1.2.7, cioè che se H è un sottogruppo astratto e chiuso allora è anche un sottogruppo di Lie. Il fatto che localmente la mappa esponenziale è un diffeomorfismo giustifica la seguente.

Definizione 1.2.11. Sia U un intorno di 0 che viene mappato in modo diffeomorfo in un intorno U' di e dalla mappa exp; si definisce la *mappa logaritmo* come l'inversa locale di exp in U' e si denota con $\log\colon U' \to U$.

Lemma 1.2.12. *Siano H un sottogruppo astratto chiuso di un gruppo di Lie G e $(h_n)_{n\in\mathbb{N}}$ una successione in $H' := \log(H \cap U')$ che converga a 0 e tale che ${}^{h_n}/_{|h_n|}$ converga a $X \in G_e$, dove la norma è data da un qualsiasi prodotto scalare. Allora $\exp(sX) \in H$ per ogni s.*

Dimostrazione. Si possono trovare degli interi m_n tali che $m_n\,|h_n| \to s$; allora

$$\exp(m_n h_n) = \exp(m_n\,|h_n|\,{}^{h_n}/_{|h_n|}) \to \exp(sX),$$

ma $\exp(m_n h_n) = (\exp(h_n))^{m_n} \in H$ e H è chiuso, quindi $\exp(sX) \in H$. □

Lemma 1.2.13. *Sia W l'insieme dei vettori sX con $s \in \mathbb{R}$ e X limite di una successione ${}^{h_n}/_{|h_n|}$ con $(h_n)_{n\in\mathbb{N}}$ come nel lemma 1.2.12; allora W è un sottospazio.*

Dimostrazione. Si deve solo dimostrare che se $X, Y \in W$, allora $X + Y \in W$: da $\exp(sX)\exp(sY) = \exp(sX + sY + \mathrm{o}(s))$, applicando il logaritmo, si scrive la funzione $\tilde{h}(s) := \log\exp(sX + sY + \mathrm{o}(s))$; ora, $1/s\tilde{h}(s)$ converge alla somma $X + Y$, quindi basta prendere $h_n := \tilde{h}(1/n)$ e applicare il lemma 1.2.12. □

Lemma 1.2.14. *L'esponenziale di W è un intorno di e in H.*

Dimostrazione. Se non fosse così, si avrebbe una successione di coppie $(X_n, Y_n) \in W \times (W^\perp \setminus \{0\})$ che tende a $(0, 0)$ e tale che $\exp(X_n)\exp(Y_n) \in H$. Ma eventualmente estraendo una sottosuccessione, si ha che $Y_n/|Y_n| \to D$ (perché la sfera unitaria è compatta); essendo H un sottogruppo astratto, da $\exp(X_n) \in H$ si ricava $\exp(Y_n) \in H$, che per i lemmi 1.2.12 e 1.2.13 implica $\exp(sD) \in H$ e $D \in W$. Ma questo è assurdo, perché $|D| = 1$, $D \in W$ e D è limite di elementi di $W^\perp$, quindi $D \in W^\perp$. □

Dimostrazione del teorema 1.2.7. $\Leftarrow$ Se H è discreto, è già automaticamente una sottovarietà regolare, altrimenti si utilizzano i tre lemmi precedenti: si considera il sottospazio W e si scrive $G_e = W \oplus W^\perp$. La mappa $W \oplus W^\perp \to G\colon (X, Y) \mapsto \exp(X)\exp(Y)$ è un diffeomorfismo locale e in particolare $\langle \exp(W) \rangle = H$, cioè la restrizione a W è una carta locale per H, che si può traslare sopra ogni suo elemento. □

1.3 Teoria delle rappresentazioni dei gruppi topologici

15.03.2007

Definizione 1.3.1. Sia G un gruppo topologico (cioè un gruppo con una topologia rispettata dalle operazioni). Una *rappresentazione finita* di G sul campo $K \in \{\mathbb{R}, \mathbb{C}\}$ è un morfismo di gruppi continuo $G \to \mathrm{GL}(V)$ dove V è uno spazio vettoriale di dimensione finita su K. Si dice anche che V è un *G-modulo*.

Definizione 1.3.2. Una *G-applicazione lineare* (o *mappa di G-moduli*) tra due G-moduli V e W è un'applicazione lineare $\varphi\colon V \to W$ tale che $\varphi(gv) = g\varphi(v)$ per ogni $v \in V$ e $g \in G$. L'insieme delle G-applicazioni lineari si denota con $\mathrm{Hom}_G(V, W)$.

Osservazione 1.3.3. Se sono date delle rappresentazioni di G, si possono costruire da queste altre rappresentazioni: se V e W sono G-moduli, $\mathrm{Hom}_K(V, W)$ è un G-modulo con $(gF)(v) := gFg^{-1}(v)$; gli invarianti di questa azione sono le G-applicazioni lineari. Se $W = K$, si ottiene la G-rappresentazione $V^\star$.

Nel caso dei gruppi finiti, può essere utile considerare la media delle azioni degli elementi di G; nel caso di gruppi topologici generici questo non è più possibile; tuttavia, per quelli compatti, si può considerare l'integrale delle azioni al variare di $g \in G$.

Sia G un gruppo topologico compatto; si suppone di avere una funzione $f\colon G \to \mathbb{R}$ continua; allora si può dimostrare l'esistenza di una mappa $f \mapsto \int_G f \in \mathbb{R}$ che abbia le proprietà di:

1. positività: $f \geq 0 \Rightarrow \int_G f \geq 0$;
2. linearità: $\int_G (\lambda f + \mu g) = \lambda \int_G f + \mu \int_G g$;
3. normalità: $\int_G 1 = 1$;

4. invarianza rispetto alla moltiplicazione a sinistra e a destra: $\int_{y\in G} f(xy) = \int_{y\in G} f(y) = \int_{y\in G} f(yx)$.

Allo stesso modo, componente per componente, si integrano le funzioni continue $f\colon G \to \mathbb{R}^n$. La misura che definisce questo integrale si chiama *misura di Haar*; per i gruppi topologici compatti si dimostra l'esistenza e anche l'unicità, se si richiede la normalità. Nel caso di gruppi topologici localmente compatti si possono integrare in modo simile le funzioni a supporto compatto.

Esempio 1.3.4. Si considera $G := \mathrm{U}(1) \approx S^1$, allora $\int_{\mathrm{U}(1)} f = \int_0^{2\pi} f(\varphi)\mathrm{d}\varphi$ dove φ è la parametrizzazione con la lunghezza d'arco.

Proposizione 1.3.5. *Sia $\vartheta\colon G \to \mathrm{GL}(V)$ una rappresentazione; sia $I := \int_{g\in G} \vartheta(g) \in \mathrm{Hom}_K(V,V)$ (I è la media degli operatori $\vartheta(g)$). Allora $I^2 = I$ e $I(V)$ è il sottospazio degli elementi di V fissati da G, cioè I è una proiezione.*

Dimostrazione. Per ogni $v \in V$, la valutazione in v, $\mathrm{Hom}_K(V,V) \to V\colon F \to F(v)$ è lineare. Allora $I(v) = (\int_{g\in G} g)v = \int_{g\in G}(gv)$, per la linearità dell'integrale. Si vuole dimostrare che per ogni $h \in G$ e $v \in V$, $hI(v) = I(v)$, ma $hI(v) = h\int_{g\in G} gv = \int_{g\in G} hgv = \int_{g\in G} gv = I(v)$, per l'invarianza a sinistra. Viceversa, se $gw = w$ per ogni $g \in G$, allora $I(w) = \int_{g\in G} gw = \int_{g\in G} ew = \mathrm{Id}\, w = w$ per la normalità. Da questi due fatti si ha facilmente che $I^2 = I$. □

Proposizione 1.3.6. *Sia G un gruppo topologico compatto e V un G-modulo su $\mathbb{C}$; allora si può trovare su V una forma hermitiana definita positiva H che è invariante rispetto all'azione di G.*

Dimostrazione. Sia L lo spazio vettoriale reale di tutte le forme hermitiane; G agisce su L definendo $gK(v,w) := K(g^{-1}v, g^{-1}w)$. Sia $H := \int_{g\in G} gK$, dove ora K è una fissata forma hermitiana definita positiva; per la proposizione 1.3.5, H è invariante a sinistra, poiché, con le notazioni della proposizione, $H = I(K)$. Quindi $gH(v,w) = H(g^{-1}v, g^{-1}w) = H(v,w)$. Per la positività dell'integrale, se K è definita positiva, anche H sarà definita positiva. □

Si può fare la stessa costruzione anche per le rappresentazioni su $\mathbb{R}$ con i prodotti scalari. Quindi se si ha un G-modulo, si può sempre pensare che G agisca tramite trasformazioni unitarie o ortogonali (a seconda che siano rappresentazioni su $\mathbb{C}$ o su $\mathbb{R}$) e si scriverà $G \to \mathrm{U}(V)$ o $G \to \mathrm{O}(V)$.

1.4 Tori

Definizione 1.4.1. Sia G un gruppo topologico e sia $g \in G$; se la chiusura di $\langle g\rangle$ è tutto G, si dirà che g è un *generatore* di G e che G è *monogenerato.*

Esercizio 1.4.2. La chiusura di un sottogruppo astratto abeliano è un sottogruppo abeliano (per continuità, prendendo successioni di elementi del sottogruppo); in particolare, se G è monogenerato, è abeliano.

Proposizione 1.4.3. *Il toro T^k è monogenerato.*

Dimostrazione. Siano $U_1, \dots, U_n, \dots$ gli aperti di una base numerabile della topologia di T^k e si pongano sul toro le coordinate indotte da $\mathbb{R}^k/\mathbb{Z}^k$; dati $\varepsilon \in \mathbb{R}^+$ e $\xi := (\xi_1, \dots, \xi_k) \in \mathbb{R}^k$, il cubo di centro ξ e lato 2ε è l'insieme

$\{ x \in T^k \mid (\forall i)\, |x_i - \xi_i| \leq \varepsilon \}$. Si scelga un cubo qualsiasi, C_0; si costruirà per induzione, a partire da C_0, una successione decrescente di cubi la cui intersezione sarà un generatore del toro.

Si suppone di aver già scelto $C_0 \supseteq \cdots \supseteq C_{m-1}$ e che C_{m-1} abbia lato $2\varepsilon_{m-1}$ e centro ξ_{m-1}; allora esiste un intero $N(m)$ tale che $2\varepsilon_{m-1} \cdot N(m) > 1$, cioè tale che il cubo di centro ξ_{m-1} e lato $2\varepsilon_{m-1} \cdot N(m)$ sia tutto il toro. A questo punto, si può trovare $C_m \subseteq C_{m-1}$ tale che $N(m) \cdot C_m \subseteq U_m$.

Sia $g \in \bigcap C_m$: allora $g^{N(m)} \in U_m$ per ogni m, il che è equivalente a dire che g genera T^k. $\square$

Definizione 1.4.4. Un *toro massimale* $T \subseteq G$ è un sottogruppo isomorfo a un toro tale che se esiste un altro toro U con $T \subseteq U \subseteq G$, si ha $T = U$.

Proposizione 1.4.5. *Dato un gruppo di Lie compatto G, la chiusura di un suo sottogruppo a un parametro non banale è un toro non banale.*

Dimostrazione. Si considera un sottogruppo a un parametro, $f(s) \coloneqq \exp(sX)$; allora la chiusura di $f(\mathbb{R})$ è un sottogruppo abeliano compatto e connesso, quindi è un toro. $\square$

Proposizione 1.4.6. *In ogni gruppo di Lie compatto non banale esiste almeno un toro massimale non banale.*

Dimostrazione. Per la proposizione 1.4.5, esiste un toro non banale; presa una catena ascendente di tori $T_1 \subseteq \cdots \subseteq T_n \subseteq \cdots$, questa dà una catena ascendente di sottospazi del tangente nell'identità, ma questo ha dimensione finita, perciò la catena deve stabilizzarsi. $\square$

20.03.2007

Dato $g \in G$, si considera il coniugio $i_g \colon G \to G$ con $i_g(h) \coloneqq ghg^{-1}$; si ha un'azione di G su G_e data da $i'_{g|G_e}$; d'altra parte la mappa $i'_{g|G_e}$ è invertibile (dato che $i_{g^{-1}} = i_g^{-1}$). L'*azione aggiunta* $\mathrm{Ad} \colon G \to \mathrm{Aut}(G_e)$ così definita è quindi un morfismo di gruppi di Lie: il fatto che sia morfismo di gruppi è ovvio, e la regolarità deriva dalla regolarità di tutte le mappe coinvolte.

Per la proposizione 1.3.6, se G è compatto, si può considerare su G_e un prodotto scalare invariante per l'azione aggiunta. Si considererà ora un gruppo di Lie compatto G con l'azione aggiunta ristretta a un toro contenuto nel gruppo. È ovvio che l'azione di ogni elemento del toro su G_e si può decomporre in spazi ortogonali di dimensione 1 e 2, in quanto $\mathrm{Ad}(g) \subseteq \mathrm{O}(n)$; si dimostra che esiste una decomposizione di questo tipo anche per tutto il toro.

Teorema 1.4.7. *Sia $T \subseteq G$ un toro; allora si può trovare una decomposizione ortogonale di G_e, $G_e = V_0 \oplus \bigoplus_{r=1}^m V_r$ tale che $\dim V_r = 2$ per $r \geq 1$, i V_i siano $\mathrm{Ad}(T)$ invarianti, T agisca su V_0 in modo banale e su V_r, $r \geq 1$, l'azione di $t \in T$ sia*

$$\mathrm{Ad}(t)_{|V_r} = \begin{pmatrix} \cos 2\pi\bar{\vartheta}_r(t) & -\sin 2\pi\bar{\vartheta}_r(t) \\ \sin 2\pi\bar{\vartheta}_r(t) & \cos 2\pi\bar{\vartheta}_r(t) \end{pmatrix},$$

con $\bar{\vartheta}_r \colon T \to \mathbb{R}/\mathbb{Z}$ un morfismo suriettivo non banale.

Dimostrazione. Sia t un generatore del toro (cioè, $\overline{\langle t \rangle} = T$); allora $\mathrm{Ad}(t) \in \mathrm{O}(G_e)$, scegliendo un prodotto scalare compatibile con l'azione. Quindi, scegliendo una base opportuna, $\mathrm{Ad}(t)$ è una matrice che ha sulla diagonale vari elementi 1 o -1 o blocchi 2×2 che rappresentano rotazioni $\alpha_n = \left(\begin{smallmatrix} \Re\alpha_n & -\Im\alpha_n \\ \Im\alpha_n & \Re\alpha_n \end{smallmatrix}\right)$

con $\|\alpha_n\| = 1$. Anche $\operatorname{Ad}(t^n) = \operatorname{Ad}(t)^n$ ha una decomposizione di questo tipo (sulla stessa base) e per continuità anche ogni elemento di T.

Ora, per ogni spazio invariante V_j, $\operatorname{Ad}_{|T} \colon T \to \mathrm{O}(V_j)$ è una mappa continua dal toro, che è connesso, a $\mathrm{O}(V_j)$ che ha due componenti connesse (di determinante $+1$ o -1). Di conseguenza l'immagine di $\operatorname{Ad}_{|T}$ è contenuta in $\mathrm{SO}(V_j)$ (perché l'identità deve andare nell'identità) e in particolare gli autovalori relativi ai sottospazi invarianti di dimensione unitaria sono tutti 1 (perché $\mathrm{SO}(\mathbb{R}) = \{1\}$).

Allora, posto V_0 il sottospazio dato dalla somma dei sottospazi fissi di dimensione 1, si ha che $\operatorname{Ad}(T)_{|V_0}$ è l'identità, mentre su V_i, $i \geq 1$, agisce con una matrice $\left(\begin{smallmatrix} \cos 2\pi\bar{\vartheta}_r(t) & -\sin 2\pi\bar{\vartheta}_r(t) \\ \sin 2\pi\bar{\vartheta}_r(t) & \cos 2\pi\bar{\vartheta}_r(t) \end{smallmatrix}\right)$, dove $\bar{\vartheta}_i \colon T \to \mathrm{SO}(V_i) \cong S^1$ e inoltre si sa che questo morfismo non è banale (altrimenti V_i confluirebbe in V_0). L'immagine di $\bar{\vartheta}_i$ è abeliana, connessa, compatta, quindi è un toro; essendo contenuta in S^1 e non potendo essere un unico punto, deve essere S^1. □

Proposizione 1.4.8. *Ogni $\bar{\vartheta}_r$ è unico a meno di segno e ordine, ossia l'insieme $\{\pm\bar{\vartheta}_1, \ldots, \pm\bar{\vartheta}_m\}$ è determinato da G e da T.*

Dimostrazione. L'insieme non dipende dalla decomposizione ortogonale e dalla base perché gli α_r sono legati alle radici del polinomio caratteristico di $\operatorname{Ad}(t)$. Scegliendo t' invece di t per costruire la decomposizione, si può presumere che entrambi siano generatori del toro; da questo si deduce che le rotazioni relative a un determinato sottospazio sono le stesse. □

Poiché T_e è semplicemente connesso, esiste un unico sollevamento $\vartheta_r \in T_e^\star$ di $\bar{\vartheta}_r \circ \exp$ a $\mathbb{R}$:

$$\begin{tikzcd} & & \mathbb{R} \arrow[d, "\pi"] \\ T_e \arrow[urr, dashed, "\vartheta_r"] \arrow[r, "\exp"'] & T \arrow[r, "\bar{\vartheta}_r"'] & \frac{\mathbb{R}}{\mathbb{Z}}; \end{tikzcd}$$

inoltre ϑ_r è un morfismo (lo è in un intorno dell'identità e si verifica che si può estendere), è lineare (quindi appartiene davvero a $T_e^\star$) e $\ker(\exp)$ deve necessariamente essere mappato in $\mathbb{Z}$ da ϑ_r.

Definizione 1.4.9. Se T è un toro massimale, $\pm\vartheta_r$ si dicono *radici* di G.

Teorema 1.4.10. *Sia G un gruppo di Lie compatto; un toro $T \subseteq G$ è massimale se e solo se $V_0 = T_e$.*

Dimostrazione. $\Leftarrow$ Sia $T' \supseteq T$ un toro; si considera $t \in T$ e si studia l'azione $\operatorname{Ad}(t)$ su T'_e. Per fare questo si calcola la derivata in 0 di $t(\exp(sX))t^{-1}$, che equivale a $\operatorname{Ad}(t)(X)$, per ogni $X \in T'_e$. Si ha

$$\begin{aligned} \operatorname{Ad}(t)(X) &= \left[\frac{\mathrm{d}}{\mathrm{d}s} t(\exp(sX))t^{-1}\right]_{s=0} = \\ &= \left[\frac{\mathrm{d}}{\mathrm{d}s} \exp(sX)\right]_{s=0} = X, \end{aligned}$$

perché $t\exp(sX)t^{-1} \in T'$ che è commutativo. Allora $T'_e \subseteq V_0 = T_e$. Essendo per ipotesi $T_e \subseteq T'_e$, si ha $T = T'$, poiché sono entrambi gruppi di Lie connessi.

$\Rightarrow$ Per assurdo, sia $X \in V_0 \backslash T_e$; si mostra che $\exp(sX)$ commuta con gli elementi di T, infatti, con lo stesso calcolo di prima, si ottiene, per ogni $t \in T$

$$\left[\frac{\mathrm{d}}{\mathrm{d}s} t \exp(sX) t^{-1}\right]_{s=0} = \mathrm{Ad}(t)(X) = X,$$

dove l'ultima uguaglianza si deve al fatto che $X \in V_0$, che è stabile; da questo si deduce che $t \exp(sX)t^{-1} = \exp(sX)$ perché sono entrambi sottogruppi a un parametro che hanno X come tangente nell'identità. Allora $\langle t, \exp(sX)\rangle$ è abeliano (i suoi generatori commutano), è connesso (è prodotto di gruppi connessi) ed è compatto (è chiuso in G che è compatto): è un toro strettamente più grande di T, assurdo. Si è dimostrato che $V_0 \subseteq T_e$; il viceversa viene ancora una volta dal calcolo precedente, da cui in particolare si ottiene che gli elementi di un toro agiscono banalmente sul suo tangente. $\square$

Esempio 1.4.11. Si considera $\mathrm{U}(n)$: un toro massimale si può cercare tra le matrici diagonali, poiché la loro commutatività è ovvia. Le matrici del tipo $\mathrm{diag}(e^{ix_1}, \dots, e^{ix_n})$ formano un T^n dentro $\mathrm{U}(n)$; si deve verificare se sia massimale. Siano $E_{r,s}$ le matrici date da $(\delta_{i,r}\delta_{j,s})_{i,j}$ (nulle a meno di un 1 in posizione (r,s)). Per $r < s$, lo spazio $V_{r,s} := \{ zE_{r,s} - \bar{z}E_{s,r} \mid z \in \mathbb{C} \}$ è invariante per $\mathrm{Ad}(T)$. Infatti, per qualsiasi gruppo di matrici, l'azione aggiunta è il coniugio di matrici: $\mathrm{Ad}(D)(X) = DXD^{-1}$. Allora se $D = \mathrm{diag}(e^{ix_1}, \dots, e^{ix_n})$, $D(zE_{r,s} - \bar{z}E_{s,r})D^{-1} = e^{i(x_r - x_s)}(zE_{r,s} - \bar{z}E_{s,r})$.

Questi $V_{r,s}$ sono $\binom{n}{2}$, quindi danno una dimensione totale di $n(n-1)$, dato che su di loro l'azione del toro è una rotazione non banale. D'altra parte, il toro ha dimensione n e l'azione sul suo tangente è banale: in tutto si sa spezzare l'azione di T su una parte di dimensione n^2 di $\mathfrak{u}(n)$. Ma $\mathfrak{u}(n)$ è dato dalle matrici antihermitiane, cioè tali che $\bar{X}^t = -X$, che sui reali hanno dimensione n^2: si è spezzato tutto il tangente.

Come conseguenza si ha che $V_0 = T_e$, quindi T è massimale. Inoltre le radici di $\mathrm{U}(n)$ sono i funzionali $x_r - x_s \colon T_e \cong \mathbb{R}^n \to \mathbb{R}$.

22.03.2007

Sia $H := \{ e^{i\lambda} I \mid \lambda \in \mathbb{R} \}$; in termini di gruppi, $\mathrm{U}(n) = \mathrm{SU}(n) \times H$. Quindi un toro massimale di $\mathrm{U}(n)$ è un toro massimale di $\mathrm{SU}(n)$ prodotto cartesiano H; la commutatività è assicurata dal fatto che H è contenuto nel centro di $\mathrm{U}(n)$.

2 Algebre di Lie

2.1 Introduzione

Definizione 2.1.1. Sia K un campo; un K-spazio vettoriale astratto $\mathfrak{g}$ si dice un'*algebra di Lie* se esiste una mappa $\mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ che associa a (X, Y) un elemento denotato $[X, Y]$ in modo che:

1. la mappa sia bilineare;

2. $[X, Y] + [Y, X] = 0$ (si suppone di non essere in caratteristica 2);

3. valga l'uguaglianza di Jacobi: $[X, [Y, Z]] + [Z, [X, Y]] + [Y, [Z, X]] = 0$.

Sono algebre di Lie, ad esempio, i gruppi di endomorfismi con il prodotto bracket ($[A, B] \coloneqq AB - BA$); oppure se M è una varietà, i campi di vettori con il prodotto $[X, Y] \coloneqq X \circ Y - Y \circ X$ sono ancora un'algebra di Lie.

Proposizione 2.1.2. *Lo spazio di tutti i campi di vettori* C^∞ *invarianti a sinistra su un gruppo di Lie* G *è un'algebra di Lie, col prodotto definito prima.*

Dimostrazione. Se π è una mappa C^∞ con $\pi\colon G \to G$, per ogni X, Y campi di vettori vale $(\pi' X)f = X(f \circ \pi)$; fissando $\pi = L_g$, se X e Y sono anche invarianti a sinistra, si ha $\pi' X = X$ e $\pi' Y = Y$, quindi $\pi'[X, Y]f = [X, Y](f \circ \pi) = XY(f \circ \pi) - YX(f \circ \pi) = X(\pi' Y)f - Y(\pi' X)f = XYf - YXf = [X, Y]f$, cioè $[X, Y]$ è invariante a sinistra. □

Definizione 2.1.3. Un *morfismo di algebre di Lie* tra $\mathfrak{g}_1$ e $\mathfrak{g}_2$ è un'applicazione lineare $\varphi\colon \mathfrak{g}_1 \to \mathfrak{g}_2$ tale che $\varphi([X, Y]) = [\varphi(X), \varphi(Y)]$.

Mimando l'azione aggiunta $\mathrm{Ad}\colon G \to \mathrm{Aut}(G_e)$, si definisce la *mappa aggiunta* $\mathrm{ad}\colon \mathfrak{g} \to \mathrm{End}(\mathfrak{g})$, con $\mathrm{ad}(X)(Y) = [X, Y]$. La mappa aggiunta è la moltiplicazione a sinistra in un'algebra di Lie ed è un morfismo di algebre di Lie, dove $\mathrm{End}(\mathfrak{g})$ ha la struttura data dal bracket tra matrici: bisogna verificare che $\mathrm{ad}([X, Y]) = [\mathrm{ad}(X), \mathrm{ad}(Y)]$, ma preso $W \in \mathfrak{g}$, si ha

$$\begin{aligned} \mathrm{ad}([X, Y])(W) &= [[X, Y], W], \\ [\mathrm{ad}(X), \mathrm{ad}(Y)](W) &= \mathrm{ad}(X)(\mathrm{ad}(Y)(W)) - \mathrm{ad}(Y)(\mathrm{ad}(X)(W)) = \\ &= [X, [Y, W]] - [Y, [X, W]]. \end{aligned}$$

I due risultati sono uguali applicando l'uguaglianza di Jacobi.

Definizione 2.1.4. Data un'algebra di Lie $\mathfrak{g}$, il *centro* di $\mathfrak{g}$ è dato dagli elementi $X \in \mathfrak{g}$ tale che $[X, Y] = 0$ per ogni $Y \in \mathfrak{g}$ e si denota con $\mathrm{Z}(\mathfrak{g})$.

Ovviamente si ottiene che il nucleo della mappa aggiunta è il centro di $\mathfrak{g}$.

Dato un campo di vettori invariante a sinistra su un gruppo di Lie G, questo è univocamente determinato dal valore che assume su G_e. Allora si può definire una struttura di algebra di Lie su G_e grazie al prodotto bracket $[X_e, Y_e] \coloneqq [X, Y]_e$, dove X e Y sono i campi di vettori invarianti a sinistra che valgono rispettivamente X_e e Y_e su G_e.

Teorema 2.1.5. *Sia* $\varphi\colon G_1 \to G_2$ *un morfismo di gruppi di Lie, allora* $\varphi'\colon \mathfrak{g}_1 \to \mathfrak{g}_2$ *è un morfismo di algebre di Lie.*

Dimostrazione. Il fatto che φ sia un morfismo di gruppi di Lie si può leggere come $\varphi \circ L_\sigma = L_{\varphi(\sigma)} \circ \varphi$ per ogni $\sigma \in G_1$. Differenziando, $\varphi' \circ L'_\sigma = L'_{\varphi(\sigma)} \circ \varphi'$. Siano X e Y i campi di vettori invarianti a sinistra su G_1 che valgono rispettivamente X_e e Y_e in $\mathfrak{g}_1$; siano inoltre W e Z i campi di vettori invarianti a sinistra che valgono rispettivamente $W_e \coloneqq \varphi'(X_e)$ e $Z_e \coloneqq \varphi'(Y_e)$ su $\mathfrak{g}_2$. Allora dall'uguaglianza ottenuta all'inizio si ricava

$$\varphi'(X_\sigma) = \varphi' \circ L'_\sigma(X_e) = L'_{\varphi(\sigma)} \circ \varphi'(X_e) = L'_{\varphi(\sigma)}(W_e) = W_{\varphi(\sigma)}$$

e allo stesso modo $\varphi'(Y_\sigma) = Z_{\varphi(\sigma)}$, cioè $\varphi'(X) = W$ e $\varphi'(Y) = Z$. Di conseguenza

$$\varphi'[X, Y] = [\varphi'(X), \varphi'(Y)] = [W, Z]$$

e valutando in e si ottiene $\varphi'[X_e, Y_e] = [W_e, Z_e] = [\varphi'(X_e), \varphi'(Y_e)]$. □

La mappa $\mathrm{Ad}\colon G \to \mathrm{Aut}(G_e)$ è un morfismo di gruppi di Lie, quindi $\mathrm{Ad}'\colon \mathfrak{g} \to \mathrm{End}(G_e)$ è un morfismo di algebre di Lie. In più, si ha il seguente.

Teorema 2.1.6. *Sia G un gruppo di Lie, allora* $\mathrm{Ad}' = \mathrm{ad}$.

Dimostrazione. Si dimostrerà solo per $G \subseteq \mathrm{GL}(V)$: si userà il fatto che per i gruppi di matrici, l'esponenziale è l'esponenziale di matrici. In questa situazione,

$$\begin{aligned}\mathrm{Ad}'(X)(Y) &= \left[\frac{\mathrm{d}}{\mathrm{d}s}\mathrm{Ad}(e^{sX})(Y)\right]_{s=0} = \left[\frac{\mathrm{d}}{\mathrm{d}s}e^{sX}Ye^{-sX}\right]_{s=0} = \\ &= \left[\frac{\mathrm{d}}{\mathrm{d}s}(Y + s[X,Y] + \mathrm{o}(s))\right]_{s=0} = [X,Y] = \mathrm{ad}(X)(Y). \qquad \square\end{aligned}$$

Per la dimostrazione generale si usa lo stesso concetto, insieme alla formula di Baker-Campbell-Hausdorff:

$$\begin{aligned}\exp(sX)\exp(sY) = \exp\Bigg(s(X+Y) + \frac{s^2}{2}[X,Y] &+ \\ + \left(\frac{1}{12}[[X,Y],Y] - \frac{1}{12}[[X,Y],X]\right)s^3 + \mathrm{o}(s^3)\Bigg).\end{aligned}$$

Si può dimostrare (si veda [Var84]) che tutti i termini che compaiono nella formula sono esprimibili come bracket (in particolare, se X e Y commutano, rimane solo il primo termine).

Osservazione 2.1.7. Applicando il teorema 1.1.10 con $\varphi = \mathrm{Ad}$ si ha $\exp(\mathrm{ad}(X)) = \mathrm{Ad}(\exp(X))$.

Si prende ora un prodotto scalare $(\bullet,\bullet)$ su G_e che sia $\mathrm{Ad}(G)$-invariante.

Proposizione 2.1.8. *Per ogni $X, Y, Z \in G_e$, vale $([Z,X],Y) = (X,[Y,Z])$.*

Dimostrazione. Grazie all'invarianza del prodotto scalare, si ha

$$(\mathrm{Ad}(g)(X), Y) = (X, \mathrm{Ad}(g^{-1})(Y)),$$

che per $g = \exp(sZ)$ diventa

$$(\mathrm{Ad}(\exp(sZ))(X), Y) = (X, \mathrm{Ad}(\exp(-sZ))(Y)).$$

Derivando rispetto a s e valutando in 0, si ottiene $(\mathrm{ad}(Z)(X), Y) = (X, \mathrm{ad}(-Z)(Y))$, cioè $([Z,X],Y) = (X,[Y,Z])$. $\square$

Teorema 2.1.9 (Hunt)**.** *Se $X, Y \in G_e$ con G compatto, esiste $\sigma \in G$ tale che $[X, \mathrm{Ad}(\sigma)(Y)] = 0$. In altre parole, esiste un elemento del gruppo che agendo su Y, lo fa commutare con X.*

Dimostrazione. Si considera $\min\{\, (X, \mathrm{Ad}(\sigma)(Y)) \mid \sigma \in G \,\}$ (che esiste perché il gruppo è compatto). Sia $h \in G$ un elemento che realizza il minimo, allora preso $Z \in G_e$ si può fare $(X, \mathrm{Ad}(\exp(sZ))(\mathrm{Ad}(h)(Y)))$. Come funzione di s è una funzione C^∞ e ha sicuramente un minimo per $s = 0$ (dato che per $s = 0$ vale $(X, \mathrm{Ad}(e)(\mathrm{Ad}(h)(Y))) = (X, \mathrm{Ad}(h)(Y))$); perciò

$$\begin{aligned}0 &= \left[\frac{\mathrm{d}}{\mathrm{d}s}(X, \mathrm{Ad}(\exp(sZ))(\mathrm{Ad}(h)(Y)))\right]_{s=0} = (X, \mathrm{ad}(Z)(\mathrm{Ad}(h)(Y))) = \\ &= (X, [Z, \mathrm{Ad}(h)(Y)]) = ([\mathrm{Ad}(h)(Y), X], Z),\end{aligned}$$

dove l'ultima uguaglianza è per la proposizione 2.1.8. Ora, Z può variare, ma la forma è definita positiva, quindi $[\mathrm{Ad}(h)(Y), X] = 0$. □

29.03.2007

Teorema 2.1.10. *Sia G un gruppo di Lie compatto; allora tutti i tori massimali sono coniugati tra loro.*

Dimostrazione. Siano T e T' tori massimali; siano $X \in T_e$ tale che $\exp(sX)$ è denso in T (basta prendere X tale che $\exp(X)$ genera T) e $X' \in T'_e$ con $\exp(sX')$ denso in T'. Per il teorema 2.1.9, esiste σ tale che $[X, \mathrm{Ad}(\sigma)(X')] = 0$: questo moralmente significa che $\mathrm{Ad}(\sigma)(X')$ sta già in T_e, altrimenti si potrebbe estendere il toro, ma questa intuizione deve essere controllata.

Si ha che $e^{\mathrm{ad}(s_1X)}(\mathrm{Ad}(\sigma)(X')) = \mathrm{Ad}(\sigma)(X')$: $\mathrm{ad}(s_1X) \in \mathrm{Aut}(G_e)$ e lo sviluppo dell'esponenziale dà $I + \mathrm{ad}(s_1X) + \cdots$, che applicato a $\mathrm{Ad}(\sigma)(X')$ annulla tutti i termini tranne l'identità. D'altra parte l'elevamento con base e è proprio la mappa exp (dato che la mappa aggiunta vive nel mondo delle matrici); quindi

$$\begin{aligned}\mathrm{Ad}(\sigma)(X') = e^{\mathrm{ad}(s_1X)}(\mathrm{Ad}(\sigma)(X')) &= \exp(\mathrm{ad}(s_1(X)))(\mathrm{Ad}(\sigma(X'))) = \\ &= \mathrm{Ad}(\exp(s_1X))(\mathrm{Ad}(\sigma)(X')) = \\ &= \left[\frac{\mathrm{d}}{\mathrm{d}s}\exp(s_1X)\exp(s\,\mathrm{Ad}(\sigma)(X'))\exp(-s_1X)\right]_{s=0}.\end{aligned}$$

In definitiva, $\exp(s_1X)\exp(s\,\mathrm{Ad}(\sigma)(X'))\exp(-s_1X) = \exp(s\,\mathrm{Ad}(\sigma)(X'))$, perché sottogruppi a un parametro che hanno lo stesso tangente in 0. Questo significa che il sottogruppo a un parametro associato al vettore $\mathrm{Ad}(\sigma)(X')$ commuta con tutto il toro: $\overline{\langle T, \exp(s\,\mathrm{Ad}(\sigma)(X'))\rangle}$ è un toro, dato che è abeliano, è connesso perché lo sono entrambi i sottogruppi ed è compatto. Inoltre contiene T e dalla massimalità si deduce che è uguale a T, cioè $\mathrm{Ad}(\sigma)(X') \in T_e$. In particolare da questa dimostrazione si ha che se due vettori commutano, commutano anche i sottogruppi a un parametro che generano.

Ora, $\exp(s\,\mathrm{Ad}(\sigma)(X')) = \sigma\exp(sX')\sigma^{-1}$ sono lo stesso sottogruppo a un parametro (derivando e valutando in 0 si ottiene nell'identità sempre il vettore $\mathrm{Ad}(\sigma)(X')$) che è contenuto in T. Siccome $T' = \overline{\{\exp(sX')\}}$, si ha che $\sigma T'\sigma^{-1} \subseteq T$, ovvero $T' \subseteq \sigma^{-1}T\sigma$: per la massimalità di T', si ha l'uguaglianza. □

Esercizio 2.1.11. Ogni elemento di G, gruppo di Lie connesso e compatto, appartiene a un toro massimale.

Soluzione. Sicuramente se l'elemento è della forma $\exp(sX)$, è contenuto in un toro che a sua volta è contenuto in un toro massimale. Bisogna però dire che exp è suriettiva, ma questo non deriva immediatamente da quanto fatto finora. Dando per scontato questo, si può scrivere $G = \bigcup_{g \in G/\mathrm{N}(T)} gTg^{-1}$, dove T è un toro massimale. □

2.2 Algebre di Lie semisemplici

Definizione 2.2.1. Un sottospazio $I \subseteq \mathfrak{g}$ è un *ideale* se per ogni $x \in \mathfrak{g}$ e $y \in I$, vale $[x, y] \in I$.

Osservazione 2.2.2. Il centro $\mathrm{Z}(\mathfrak{g})$ è un ideale; il nucleo di un morfismo di algebre di Lie è un ideale; il quoziente di un'algebra di Lie per un suo ideale è un'algebra di Lie.

Definizione 2.2.3. Un'algebra $\mathfrak{g}$ si dice *semplice* se non ha ideali propri eccetto 0 e $\mathfrak{g}$ e non è abeliana[5], cioè $[\mathfrak{g}, \mathfrak{g}] \neq \{0\}$.

Osservazione 2.2.4. Il concetto di algebra semplice è legato all'irriducibilità dell'azione della mappa aggiunta di $\mathfrak{g}$ su se stessa.

Si è già visto che un'algebra di Lie associata a un gruppo compatto ammette una forma bilineare simmetrica invariante (cioè tale che $([X,Y],Z) + (Y,[X,Z]) = 0$) definita (positiva o negativa). Si vorrà dimostrare che un'algebra $\mathfrak{g}$ che ammette una forma di questo tipo è del tipo $\mathrm{Z}(\mathfrak{g}) \oplus \mathfrak{g}_1 \oplus \cdots \oplus \mathfrak{g}_k$ con $\mathfrak{g}_i$ algebre semplici.

Proposizione 2.2.5. *Se $\mathfrak{g}$ è un'algebra di Lie che ammette una forma bilineare simmetrica invariante definita, allora ogni ideale S in $\mathfrak{g}$ è in somma diretta[6] (esiste un ideale T tale che $\mathfrak{g} = S \oplus T$).*

Dimostrazione. Si sceglie $T = S^{\perp}$, rispetto alla forma bilineare. Per l'invarianza della forma, si dimostra che T è un ideale. Infatti, siano $t \in T$ e $x \in \mathfrak{g}$, con $x = t_x + s_x$, $t_x \in T$ e $s_x \in S$; allora $[t,x] = [t,t_x] + [t,s_x]$; grazie alla proposizione 2.1.8 e al fatto che S è un ideale, si mostra che entrambi appartengono a T: preso un qualsiasi $s \in S$, per il primo si ha $(s,[t,t_x]) = ([t_x,s],t) = 0$, dato che $[t_x,s] \in S$; per il secondo, $(s,[t,s_x]) = ([s_x,s],t) = 0$, poiché $[s_x,s] \in S$. □

Teorema 2.2.6. *Sia $\mathfrak{g}$ un'algebra di Lie che ammette una forma bilineare simmetrica invariante definita, allora $\mathfrak{g} = R_0 \oplus R_1 \oplus \cdots \oplus R_k$, dove $R_0 = \mathrm{Z}(\mathfrak{g})$ e $R_1, \ldots, R_k$ sono ideali semplici. Inoltre lo spezzamento è unico, cioè l'insieme $\{R_1, \ldots, R_k\}$ è univocamente determinato.*

Dimostrazione. Sicuramente $\mathrm{Z}(\mathfrak{g})$ è un ideale; allora $\mathfrak{g} = \mathrm{Z}(\mathfrak{g}) \oplus \mathrm{Z}(\mathfrak{g})^{\perp}$. L'ortogonale ha centro banale; si prosegue dimostrando l'asserto per induzione tra le algebre con una forma bilineare simmetrica invariante definita e con centro banale: infatti, se un'algebra A di questo tipo è semplice si termina; se non è semplice, ha un ideale non banale, $R_1 \subseteq A$; allora $A = R_1 \oplus R_1^{\perp}$. Questi due ideali hanno ancora centro banale, quindi si prosegue per induzione.

Per l'unicità, se $\mathfrak{g} = \mathrm{Z}(\mathfrak{g}) \oplus R_1 \oplus \cdots \oplus R_k = \mathrm{Z}(\mathfrak{g}) \oplus R'_1 \oplus \cdots \oplus R'_l$, per ogni $a \in R'_1 \setminus \{0\}$, esiste $b \in R'_1$ tale che $[a,b] \neq 0$ (perché il centro di R'_1 è banale). Si può scomporre b come $b_0 + \cdots + b_k$, con $b_i \in R_i$; allora

$$0 \neq [a,b] = [a,b_0] + [a,b_1] + \cdots + [a,b_k].$$

Sia r tale che $[a,b_r] \neq 0$; allora $0 \neq [a,b_r] \in R_r \cap R'_1$, cioè $R'_1 = R_r$ per la semplicità. Allo stesso modo si trova una corrispondenza per tutti gli ideali. □

Definizione 2.2.7. Un'algebra che si spezza come somma diretta di ideali semplici si dice *semisemplice*; un'algebra di Lie che si spezza come somma diretta del centro e di una sottoalgebra semisemplice si dice *riduttiva*.

[5] Se un'algebra senza ideali non banali ha dimensione maggiore di 1 sicuramente non è abeliana (altrimenti una sottoalgebra di dimensione inferiore sarebbe un ideale); l'unico caso che elimina questa richiesta sono algebre abeliane di dimensione 1.

[6] Lo spezzamento è tra ideali, non solo tra sottospazi vettoriali: in particolare vale $[s,t] \in S \cap T = \{0\}$ per ogni $s \in S$ e $t \in T$.

Data un'algebra di Lie $\mathfrak{g}$, si introduce una forma bilineare simmetrica su $\mathfrak{g}$, detta *forma di Killing*: dati $X, Y \in \mathfrak{g}$, si pone $k(X, Y) \coloneqq \mathrm{Tr}(\mathrm{ad}(X) \circ \mathrm{ad}(Y))$. Si può dimostrare facilmente che k è invariante: da

$$\mathrm{ad}([X, Y]) = \mathrm{ad}(X) \circ \mathrm{ad}(Y) - \mathrm{ad}(Y) \circ \mathrm{ad}(X),$$

e dal fatto che la traccia è invariante per permutazioni cicliche, ponendo $\alpha \coloneqq \mathrm{ad}(X)$, $\beta \coloneqq \mathrm{ad}(Y)$ e $\gamma \coloneqq \mathrm{ad}(Z)$ si ha

$$\begin{aligned} k([X, Y], Z) + k(Y, [X, Z]) &= \mathrm{Tr}(\mathrm{ad}([X, Y]) \circ \gamma) + \mathrm{Tr}(\beta \circ \mathrm{ad}([X, Z])) = \\ &= \mathrm{Tr}(\alpha \circ \beta \circ \gamma - \cancel{\beta \circ \alpha \circ \gamma} + \cancel{\beta \circ \alpha \circ \gamma} - \beta \circ \gamma \circ \alpha) = \\ &= \mathrm{Tr}(\alpha \circ \beta \circ \gamma - \beta \circ \gamma \circ \alpha) = 0. \end{aligned}$$

Osservazione 2.2.8. Un automorfismo φ dell'algebra di Lie $\mathfrak{g}$, preserva k, cioè $k(\varphi(X), \varphi(Y)) = k(X, Y)$; infatti:

$$\begin{aligned} k(\varphi(X), \varphi(Y)) &= \mathrm{Tr}(\mathrm{ad}(\varphi(X)) \circ \mathrm{ad}(\varphi(Y))) = \mathrm{Tr}([\varphi(X), [\varphi(Y), \bullet]]) = \\ &= \mathrm{Tr}(\varphi([X, \varphi^{-1}[\varphi(Y), \bullet]])) = \mathrm{Tr}(\varphi([X, [Y, \varphi^{-1}(\bullet)]])) = \\ &= \mathrm{Tr}(\varphi \circ \mathrm{ad}(X) \circ \mathrm{ad}(Y) \circ \varphi^{-1}) = \mathrm{Tr}(\mathrm{ad}(X) \circ \mathrm{ad}(Y)) = \\ &= k(X, Y). \end{aligned}$$

Definizione 2.2.9. Data una base $(u_1, \ldots, u_n)$ di $\mathfrak{g}$, una *costante di struttura* è $c^i_{j,k} \coloneqq [u_j, u_k]^i$, la i-esima coordinata di $[u_j, u_k]$.

Esercizio 2.2.10. Da $[X, Y] = -[Y, X]$ e da Jacobi, si dimostra che $c^i_{j,k} = -c^i_{k,j}$ e $c^p_{i,s} c^s_{j,k} + c^p_{j,s} c^s_{k,i} + c^p_{k,s} c^s_{i,j} = 0$. Se la base è ortonormale rispetto alla forma bilineare simmetrica invariante definita, si ottiene (usando $c_{i,j,k} \coloneqq c^i_{j,k}$): $c_{i,j,k} = c_{j,k,i} = c_{k,i,j} = -c_{j,i,k} = -c_{k,j,i} = -c_{i,k,j}$, grazie all'invarianza della forma.

Teorema 2.2.11. *Sia $\mathfrak{g}$ un'algebra di Lie dotata di una forma bilineare simmetrica invariante definita. Allora $\mathrm{Z}(\mathfrak{g}) = \mathrm{Rad}(k)$*[7]*, dove k è la forma di Killing.*

Dimostrazione. Fissata una base $(u_1, \ldots, u_n)$ di $\mathfrak{g}$, si scrive ogni $a \in \mathfrak{g}$ come $a = a^1 u_1 + \cdots + a^n u_n$; allora

$$[a, b]^i = \sum_{j,k} a^j b^k [u_j, u_k]^i = \sum_{j,k} a^j b^k c^i_{j,k}.$$

Esplicitando la matrice di $\mathrm{ad}(a)$, si dimostra che $k(a, a) = -\sum_{i,j} \left(\sum_\alpha c_{i,\alpha,j} a^\alpha\right)^2$: in particolare, la forma di Killing è semidefinita negativa. Se $a \in \mathrm{Rad}(k)$, ogni quadrato deve essere nullo, cioè $\sum_\alpha c_{i,\alpha,j} a^\alpha = 0$, da cui $[a, b]^i = \sum_{j,\alpha} (c_{i,\alpha,j} a^\alpha) b^j = 0$, dunque $a \in \mathrm{Z}(\mathfrak{g})$. Il viceversa è banale, dato che se $a \in \mathrm{Z}(\mathfrak{g})$ l'applicazione $\mathrm{ad}(a)$ è nulla. □

17.04.2007

Il gruppo $\mathrm{Aut}(\mathfrak{g})$ è il gruppo degli automorfismi di $\mathfrak{g}$ come algebra di Lie; si può vedere dentro $\mathrm{GL}(\mathfrak{g})$, il gruppo di tutti gli automorfismi lineari di $\mathfrak{g}$, e ci si può chiedere chi sia $\mathrm{Aut}(\mathfrak{g})_e$. Se $D \in \mathrm{Aut}(\mathfrak{g})_e$, $e^{sD} \in \mathrm{Aut}(\mathfrak{g})$ per ogni $s \in \mathbb{R}$, da cui $e^{sD}([X, Y]) = [e^{sD} X, e^{sD} Y]$ per ogni $X, Y \in \mathfrak{g}$; derivando e valutando in 0, si ottiene $D([X, Y]) = [D(X), Y] + [X, D(Y)]$.

[7] Il *radicale* di una forma bilineare k è il luogo dei vettori v tali che $k(v, w) = 0$ per ogni w.

Definizione 2.2.12. Un endomorfismo lineare D che soddisfa la relazione $D([X,Y]) = [D(X),Y] + [X,D(Y)]$ è detto *derivazione* di $\mathfrak{g}$. L'insieme delle derivazioni si indica con $\mathrm{Der}(\mathfrak{g})$.

Dunque $\mathrm{Aut}(\mathfrak{g}) \subseteq \mathrm{Der}(\mathfrak{g})$. Viceversa, se D è una derivazione, si osserva che

$$D^k([X,Y]) = \sum_{i+j=k} \frac{k!}{i!j!}[D^i(X), D^j(Y)],$$

da cui $e^{sD}([X,Y]) = [e^{sD}(X), e^{sD}(Y)]$, dato che si può riscrivere la formula come

$$\frac{D^k([X,Y])}{k!} = \sum_{i+j=k} \left[\frac{D^i(X)}{i!}, \frac{D^j(Y)}{j!}\right].$$

In definitiva, si ha l'uguaglianza $\mathrm{Der}(\mathfrak{g}) = \mathrm{Aut}(\mathfrak{g})_e$.

Teorema 2.2.13. *Sia* $\mathfrak{g}$ *un'algebra di Lie su cui la forma di Killing è definita negativa. Allora il gruppo* $\mathrm{Aut}(\mathfrak{g})$*, degli automorfismi di* $\mathfrak{g}$ *come algebra di Lie, è compatto e la sua algebra di Lie,* $\mathrm{Aut}(\mathfrak{g})_e$*, coincide con* $\mathrm{ad}(\mathfrak{g})$*. Inoltre,* $\mathfrak{g} \cong \mathrm{ad}(\mathfrak{g})$ *e sia* $\mathrm{Aut}(\mathfrak{g})$ *che la sua componente connessa contenente l'identità hanno centro banale.*

Dimostrazione. L'insieme degli automorfismi come spazio vettoriale che preservano la forma di Killing è $\mathrm{O}(n)$, dato che k è definita negativa; in particolare, dall'osservazione 2.2.8 si ha che gli automorfismi di $\mathfrak{g}$ come algebra di Lie preservano k, quindi $\mathrm{Aut}(\mathfrak{g}) \subseteq \mathrm{O}(n)$.

Ora, $\mathrm{Aut}(\mathfrak{g})$ è un sottogruppo chiuso di $\mathrm{O}(n)$, che è compatto, quindi è compatto. Si vuole dimostrare che $\mathrm{Der}(\mathfrak{g}) = \mathrm{ad}(\mathfrak{g})$. Innanzitutto $\mathrm{ad}(\mathfrak{g}) \subseteq \mathrm{Der}(\mathfrak{g})$ per Jacobi:

$$\begin{aligned}\mathrm{ad}(X)([Y,Z]) &= [X,[Y,Z]] = [[X,Y],Z] + [Y,[X,Z]] = \\ &= [\mathrm{ad}(X)(Y), Z] + [Y, \mathrm{ad}(X)(Z)].\end{aligned}$$

Inoltre, $\mathrm{ad}(\mathfrak{g})$ è un ideale di $\mathrm{Der}(\mathfrak{g})$, infatti per ogni derivazione φ, si ha

$$\begin{aligned}[\varphi, \mathrm{ad}(X)] &= \varphi \circ \mathrm{ad}(X) - \mathrm{ad}(X) \circ \varphi = \varphi([X, \bullet]) - [X, \varphi(\bullet)] = \\ &= [\varphi(X), \bullet] = \mathrm{ad}(\varphi(X)).\end{aligned}$$

L'ideale $\mathrm{ad}(\mathfrak{g})$ è chiamato *ideale delle derivazioni interne* di $\mathfrak{g}$.

Allora $\mathrm{Der}(\mathfrak{g}) = \mathrm{ad}(\mathfrak{g}) \oplus Q$, dove Q è un altro ideale di $\mathrm{Der}(\mathfrak{g})$. Si vuole dimostrare che $Q = \{0\}$: siano $q \in Q$ e $X \in \mathfrak{g}$, allora $\mathrm{ad}(q(X)) = [q, \mathrm{ad}(X)] \in Q \cap \mathrm{ad}(\mathfrak{g}) = 0$; quindi $0 = \mathrm{ad}(q(X))(Y) = [q(X), Y]$ per ogni $Y \in \mathfrak{g}$, cioè $q(X) \in \mathrm{Z}(\mathfrak{g})$. Ma il centro di $\mathfrak{g}$ è banale perché k è definita negativa, perciò $q(X) = 0$ per ogni $X \in \mathfrak{g}$, cioè $q = 0$.

Avendo $\mathfrak{g}$ centro banale (perché la forma di Killing è definita negativa), $\ker \mathrm{ad} = 0$, da cui $\mathfrak{g} \cong \mathrm{ad}(\mathfrak{g})$. Siano ora $\mathrm{Aut}(\mathfrak{g})^e$ la componente connessa di $\mathrm{Aut}(\mathfrak{g})$ contenente l'identità, $\varphi \in \mathrm{Z}(\mathrm{Aut}(\mathfrak{g})^e)$ e $X \in \mathfrak{g}$. Si considera $e^{s\,\mathrm{ad}(X)} \in \mathrm{Aut}(\mathfrak{g})^e$: derivando rispetto a s e valutando in 0 la relazione $\varphi e^{s\,\mathrm{ad}(X)} \varphi^{-1} = e^{s\,\mathrm{ad}(X)}$ si ottiene $\varphi\,\mathrm{ad}(X)\varphi^{-1} = \mathrm{ad}(X)$, cioè $\mathrm{ad}(\varphi(X)) = \mathrm{ad}(X)$ (perché $\varphi\,\mathrm{ad}(X)\varphi^{-1}(Y) = \varphi([X, \varphi^{-1}(Y)]) = [\varphi(X), Y]$). Dall'iniettività di ad, si ha $\varphi(X) = X$ per ogni X, cioè $\varphi = \mathrm{Id}$. $\square$

Corollario 2.2.14. *Un'algebra di Lie $\mathfrak{g}$ è l'algebra di Lie di un gruppo compatto se e solo se $\mathfrak{g}$ ammette una forma bilineare simmetrica invariante definita.*

Dimostrazione. La prima implicazione è già stata dimostrata nella proposizione 1.3.6; se invece $\mathfrak{g}$ ammette una forma di quel tipo, allora, per il teorema 2.2.6, $\mathfrak{g} = \mathrm{Z}(\mathfrak{g}) \oplus R_1 \oplus \cdots \oplus R_k$, dove $R_1 \oplus \cdots \oplus R_k$ è la parte semisemplice; a questo punto si può prendere $G \coloneqq {}^{\mathrm{Z}(\mathfrak{g})}/_{\mathbb{Z}^{\dim \mathrm{Z}(\mathfrak{g})}} \times \mathrm{Aut}(R_1 \oplus \cdots \oplus R_k)$. Infatti G è compatto (il toro è compatto, per la parte semisemplice si usa il teorema 2.2.13) e $G_e = \mathfrak{g}$: per la parte torale è chiaro, per la parte semisemplice si applica di nuovo il teorema 2.2.13 a $R_1 \oplus \cdots R_k$, notando che essendo semisemplice ha centro banale, quindi ammettendo anche la forma invariante definita (la restrizione di quella su $\mathfrak{g}$), la forma di Killing è definita negativa. □

Corollario 2.2.15. *Un'algebra di Lie reale $\mathfrak{g}$ è contemporaneamente semisemplice e* compatta *(cioè algebra di Lie di un gruppo compatto) se e solo se la forma di Killing è definita negativa.*

Dimostrazione. $\Rightarrow$ Per il corollario 2.2.14, se $\mathfrak{g}$ è compatta ammette una forma bilineare simmetrica invariante definita; se è anche semisemplice, in particolare $\mathrm{Z}(\mathfrak{g})$ è banale, da cui per il teorema 2.2.11, k è definita negativa.

$\Leftarrow$ Se k è definita negativa, $\mathfrak{g}$ ammette una forma bilineare simmetrica invariante definita (k stessa), perciò per il corollario 2.2.14 $\mathfrak{g}$ è compatta. Ammettendo la forma, per il teorema 2.2.6, $\mathfrak{g}$ è riduttiva, ma dal teorema 2.2.11 si ha che il centro è banale, perciò $\mathfrak{g}$ è semisemplice.

□

2.3 Teoria delle rappresentazioni delle algebre di Lie

Sia G un gruppo topologico compatto e V una G-rappresentazione (un G-modulo) $G \to \mathrm{GL}(V)$.

Definizione 2.3.1. Un G-modulo V si dice *irriducibile* se non ha sottomoduli propri.

Teorema 2.3.2. *Sia $K \in \{\mathbb{R}, \mathbb{C}\}$; ogni rappresentazione V di G su K è somma diretta di rappresentazioni irriducibili.*

Dimostrazione. Se V è irriducibile non c'è nulla da dimostrare. Se V non è irriducibile, esiste un sottomodulo proprio L. Per la proposizione 1.3.6, si considera un prodotto scalare invariante per G. Allora V si decompone come $L \oplus L^\perp$, dove l'ortogonale è fatto rispetto al prodotto scalare, e si può procedere per induzione sulla dimensione. □

Osservazione 2.3.3. Nel caso che il gruppo non sia compatto, il teorema non vale. Per esempio, sia $H \coloneqq \left\{ \left(\begin{smallmatrix} \alpha & \beta \\ 0 & \gamma \end{smallmatrix} \right) \mid \alpha, \beta, \gamma \in \mathbb{C}, \alpha\gamma \neq 0 \right\}$: H non è compatto, $\mathbb{C}^2$ è un H-modulo e $L \coloneqq \left\{ \left(\begin{smallmatrix} \delta \\ 0 \end{smallmatrix} \right) \mid \delta \in \mathbb{C} \right\}$ è l'unico sottomodulo proprio di $\mathbb{C}^2$. Infatti, se $\Gamma \neq L$ fosse un sottomodulo, allora $\left(\begin{smallmatrix} \varepsilon \\ 1 \end{smallmatrix} \right) \in \Gamma$ per qualche $\varepsilon \in \mathbb{C}$, da cui $H\Gamma = \mathbb{C}^2$, cioè $\Gamma = \mathbb{C}^2$.

Lemma 2.3.4 (Schur)**.** *Sia G un gruppo topologico; allora:*

1. *se $f \colon V \to W$ è una G-applicazione lineare tra due G-moduli irriducibili, f è nulla oppure un isomorfismo;*

2. *se V è un G-modulo irriducibile su $\mathbb{C}$ e f è una G-applicazione $f\colon V \to V$, $f = \lambda \operatorname{Id}$ per un certo $\lambda \in \mathbb{C}$.*

Dimostrazione. 1. Si ha che $\ker(f)$ e $\operatorname{Im}(f)$ sono G-sottomoduli, quindi $\ker(f) \in \{\{0\}, V\}$ e $\operatorname{Im}(f) \in \{\{0\}, W\}$.

2. Si sa che sui complessi sicuramente esistono $v \in V \setminus \{0\}$ e $\lambda \in \mathbb{C}$ tali che $f(v) = \lambda v$. Ora, $f - \lambda \operatorname{Id}\colon V \to V$ è una mappa di G-moduli con nucleo non banale, da cui per il primo punto $f = \lambda \operatorname{Id}$. □

Osservazione 2.3.5. In particolare, $\operatorname{Hom}_G(V, W) = 0$ se V e W sono irriducibili non isomorfi; $\operatorname{Hom}_G(V, V)$ ha dimensione 1 se si è su $\mathbb{C}$.

19.04.2007

Teorema 2.3.6. *Siano G un gruppo topologico e V un G-modulo; se $V = \bigoplus n_i V_i = \bigoplus m_i V_i$ con V_i irriducibili; allora $n_i = m_i$ per ogni i.*

Dimostrazione. Si considera V_j: $\operatorname{Hom}_G(V_j, V)$ si può leggere sia come $\operatorname{Hom}_G(V_j, \bigoplus n_i V_i) = \bigoplus n_i \operatorname{Hom}_G(V_j, V_i) = n_j \operatorname{End}_G(V_j)$ che come $\operatorname{Hom}_G(V_j, \bigoplus m_i V_i) = \bigoplus m_i \operatorname{Hom}_G(V_j, V_i) = m_j \operatorname{End}_G(V_j)$, grazie al lemma di Schur; quindi $m_j = n_j$. □

Osservazione 2.3.7 (Trucco unitario). Si considerano rappresentazioni complesse di $\mathfrak{sl}(n, \mathbb{C})$ e si vuole sapere se ammettono una decomposizione in rappresentazioni irriducibili. Una rappresentazione di $\mathfrak{sl}(n, \mathbb{C})$ è un morfismo di algebre di Lie $\mathfrak{sl}(n, \mathbb{C}) \to \operatorname{End}(V)$. Ora, $\mathfrak{su}(n) \subseteq \mathfrak{sl}(n, \mathbb{C})$ e in particolare $\mathfrak{su}(n) \oplus i\,\mathfrak{su}(n) = \mathfrak{sl}(n, \mathbb{C})$ (si dice che $\mathfrak{su}(n)$ è una *forma reale* di $\mathfrak{sl}(n, \mathbb{C})$).

Per applicare il trucco unitario si osserva che:

1. V è un $\mathfrak{su}(n)$-modulo (con la restrizione, chiamata $\rho\colon \mathfrak{su}(n) \to \operatorname{End}(V)$);

2. V è un $\mathrm{SU}(n)$-modulo con $\tilde{\rho}\colon \mathrm{SU}(n) \to \operatorname{End}(V)$, dove $\tilde{\rho}$ è tale che $\mathrm{d}\tilde{\rho} = \rho$, cioè $e^{\rho(sX)} = \tilde{\rho}(e^{sX})$: definendo

$$\tilde{\rho}(e^{sX}) := e^{s\rho(X)} = I + s\rho(X) + {}^{s^2}\!/_2 \rho(X)^2 + \cdots,$$

rimane da verificare che $\tilde{\rho}$ sia una mappa tra gruppi di Lie, cioè che $\tilde{\rho}(e^{sX} e^{tY}) = \tilde{\rho}(e^{sX})\tilde{\rho}(e^{tY})$; ma da una parte,

$$\tilde{\rho}(e^{sX} e^{tY}) = \tilde{\rho}(I + sX + tY + [sX, tY] + \cdots),$$

dall'altra

$$\tilde{\rho}(e^{sX})\tilde{\rho}(e^{tY}) = (I + s\rho(X) + \cdots)(I + t\rho(Y) + \cdots);$$

quindi non si può verificarlo in questo modo; in realtà, si dimostra che il sollevamento $\tilde{\rho}$ esiste nel caso che il gruppo di partenza sia semplicemente connesso, e se esiste è unico; in questo caso, $\mathrm{SU}(n)$ è semplicemente connesso, perciò il sollevamento esiste;

3. $V = V_1 \oplus \cdots \oplus V_k$ come $\mathrm{SU}(n)$-modulo (perché $\mathrm{SU}(n)$ è compatto);

4. i V_j sono anche $\mathfrak{su}(n)$-moduli (si deve mostrare che per $X \in \mathfrak{su}(n)$, $XV_j \subseteq V_j$, che si ottiene derivando e valutando in 0 l'espressione $e^{sX} V_j \subseteq V_j$);

5. V_j è anche un $(\mathfrak{su}(n) \oplus i\,\mathfrak{su}(n))$-modulo estendendo per linearità l'azione, cioè è un $\mathfrak{sl}(n, \mathbb{C})$-modulo.

Quindi V è somma diretta di $\mathfrak{sl}(n, \mathbb{C})$-moduli, irriducibili: se ci fosse un $\mathfrak{sl}(n, \mathbb{C})$-sottomodulo proprio di un V_j, si ricaverebbe un $\mathrm{SU}(n)$-sottomodulo proprio di V_j, che è impossibile per costruzione.

Il trucco unitario funziona ogniqualvolta si considerano le rappresentazione di un'algebra di Lie che ammette una forma reale compatta.

Si cercano le rappresentazioni irriducibili di $\mathfrak{sl}(2, \mathbb{C})$. Si pongono $e := \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$, $f := \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$, $h := \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$; valgono $[e, f] = h$, $[h, e] = 2e$, $[h, f] = -2f$. Queste relazioni permettono di determinare il prodotto in $\mathfrak{sl}(2, \mathbb{C})$, dato che questa algebra è generata da tre elementi. Sia V un $\mathfrak{sl}(2, \mathbb{C})$-modulo complesso e sia $v \in V$ un autovettore per h di autovalore λ. Si considera $W := \left\langle v, ev, e^2v, \dots, fv, f^2v, \dots \right\rangle$. Anche ev è un autovettore per h: $hev = [h, e]v + ehv = 2ev + \lambda ev = (\lambda + 2)ev$ (in particolare applicando e, l'autovalore aumenta di 2); allo stesso modo, $hfv = (\lambda - 2)fv$. Quindi W è generato da autovettori di h con autovalori distinti.

Per il trucco unitario applicato a V, esiste una rappresentazione W' tale che $V = W \oplus W'$. Si può ripetere il procedimento su W', il che mostra che entrambi hanno una base di autovettori per h.

Gli $e^t v$ si annullano prima o poi, altrimenti W avrebbe dimensione infinita, essendo generato da infiniti autovettori con autovalori diversi; di conseguenza esiste certamente un autovettore non nullo v per h tale che $ev = 0$. Un tale vettore si dice *vettore di peso più alto* per h e λ si dice *peso* di v. Le rappresentazioni irriducibili saranno caratterizzate da queste quantità.

Teorema 2.3.8. *Siano V irriducibile, v un vettore di peso più alto per h di peso γ, $v_{-1} := 0$, $v_0 := v$ e $v_i := {}^1\!/\!_{i!} f^i v_0$. Allora valgono $hv_i = (\gamma - 2i)v_i$, $fv_i = (i + 1)v_{i+1}$, $ev_i = (\gamma - i + 1)v_{i-1}$ per ogni $i \geq 0$.*

Queste relazioni (che sono ovvie a meno dell'azione di e, che si dimostra essere quella per induzione) mostrano che $\langle\, v_i \mid i \geq 0 \,\rangle$ è un sottomodulo, cioè, per l'irriducibilità di V, $\langle\, v_i \mid i \geq 0 \,\rangle = V$. Inoltre, la dimensione di $\langle\, v_i \mid i \geq 0 \,\rangle$ è $m+1$, dove m è il massimo indice per cui $v_m \neq 0$, perché tutti i v_i non nulli hanno autovalori diversi rispetto a h. Però dal teorema si ha anche $(\gamma - m - 1 + 1)v_m = ev_{m+1} = 0$, cioè $\gamma = m \in \mathbb{N}$ e $\dim V = \gamma + 1$.

Teorema 2.3.9. *Le rappresentazioni irriducibili di $\mathfrak{sl}(2, \mathbb{C})$ sono caratterizzate da un intero $m \in \mathbb{N}$. Sia V_m la rappresentazione associata a m, allora $\dim V_m = m + 1$ e il vettore di peso massimale rispetto a h è un autovettore di autovalore m.*

Inoltre, esiste per ogni m una rappresentazione irriducibile di dimensione $m + 1$, costruendo a mano lo spazio V_m e le azioni di e, f e h e verificando che queste soddisfano le relazioni di $\mathfrak{sl}(2, \mathbb{C})$ ($[h, e] = 2e$, $[h, f] = -2f$, $[e, f] = h$).

Corollario 2.3.10. *Data una rappresentazione L di $\mathfrak{sl}(2, \mathbb{C})$, il numero delle sue componenti irriducibili è $\dim(L_0) + \dim(L_1)$, dove L_i è l'autospazio di i.*

Questo è vero perché ogni rappresentazione irriducibile aggiunge una dimensione o a L_0 (se il peso massimale è pari) o a L_1 (se è dispari).

03.05.2007

2.4 Algebre risolubili, radicale e teorema di Lie

Sia L un'algebra di Lie; si definiscono per induzione delle algebre di Lie $L^{(i)}$ ponendo

$$L^{(0)} := L,$$
$$L^{(i+1)} := [L^{(i)}, L^{(i)}];$$

si ha $L^{(0)} \supseteq L^{(1)} \supseteq \cdots \supseteq L^{(i)} \supseteq \cdots$.

Definizione 2.4.1. Nella notazione precedente, L si dice *risolubile* se esiste $n \in \mathbb{N}$ tale che $L^{(n)} = 0$.

Esempio 2.4.2. 1. Se L è abeliana, allora è risolubile.

2. Se L è semisemplice, $L = I_1 \oplus \cdots \oplus I_r$ con I_j ideale semplice, allora $[I_j, I_j] = I_j$ (il prodotto è un ideale e non può essere 0 perché I_j è semplice, quindi non abeliano) e $[L, L] = L$; in particolare non è risolubile.

3. Le matrici triangolari superiori su un campo sono una sottoalgebra di Lie (cioè sono chiuse rispetto al bracket) e sono fatte da $D \oplus U$, con D le matrici diagonali e U le strettamente triangolari superiori; questo è il prototipo di tutte le algebre risolubili.

Esercizio 2.4.3. 1. Se L è risolubile, lo sono anche tutte le sue sottoalgebre e le sue immagini tramite morfismo.

2. Se I è un ideale risolubile di L e L/I è risolubile, allora L è risolubile.

3. Se I e J sono ideali risolubili, anche $I + J$ è risolubile.

Grazie al punto 3 dell'esercizio, esiste un ideale risolubile massimale (la somma di tutti gli ideali risolubili), che viene chiamato *radicale* di L e denotato con $\mathrm{Rad}(L)$

Esercizio 2.4.4. Il radicale di L è nullo se e solo se L non ha ideali abeliani non banali.

Osservazione 2.4.5. Usualmente, la definizione di semisemplicità si dà a partire dall'ideale radicale: L si dice semisemplice se il suo radicale è nullo.

Esercizio 2.4.6. Calcolare la forma di Killing k per $\mathfrak{sl}(n, \mathbb{R})$.

Teorema 2.4.7 (Lie)**.** *Sia L una sottoalgebra risolubile di $\mathfrak{gl}(V)$, dove V è uno spazio vettoriale di dimensione finita su $\mathbb{C}$. Se $V \neq 0$, allora contiene un autovettore comune a tutti gli elementi di L.*

Dimostrazione. Per induzione su $\dim L$: se $\dim L = 0$, non c'è nulla da dimostrare. Se $\dim L > 0$ e si suppone che l'asserto valga per algebre di dimensione fino a $\dim L - 1$, si prende un ideale K di codimensione 1 in L. Questo è possibile: per esempio si può considerare $L/[L, L]$, che è abeliana e non nulla, altrimenti L non sarebbe risolubile; essendo non nulla, ha dimensione almeno 1 e per l'abelianità si può trovare un suo ideale $\bar{K} \subseteq L/[L, L]$ di codimensione 1 (tutti i sottospazi di un'algebra abeliana sono ideali); a questo punto, si prende come K la preimmagine di $\bar{K}$ tramite la proiezione al quoziente.

Il K ottenuto è risolubile; per ipotesi induttiva, sia v un autovettore comune per gli elementi di K, cioè per ogni $X \in K$, $Xv = \lambda(X)v$ con $\lambda\colon K \to \mathbb{C}$ lineare. Sia $W \coloneqq \{\, w \in V \mid (\forall X \in K) Xw = \lambda(X)w \,\}$ (in particolare $v \in W \neq 0$).

Si ha $L = K + \mathbb{C}Z$ e a meno di ipotizzare che $LW \subseteq W$, si può prendere un $v_0 \in W$ che è autovettore per $Z_{|W}$ e che sarà l'autovettore comune cercato.

Rimane da dimostrare che $LW \subseteq W$: sia $w \in W$ e sia $X \in L$. Preso $Y \in K$, vale:

$$YXw = [Y, X]w + XYw = \lambda([Y, X])w + \lambda(Y)Xw.$$

Ci si riduce perciò a dimostrare che per ogni $X \in L$ e per ogni $Y \in K$, si ha $\lambda([X, Y]) = 0$. Si fissa $w \in W$ e si considera la successione $w, Xw, X^2w, \ldots$; sia n il più piccolo intero tale che i vettori $w, \ldots, X^n w$ siano dipendenti. Si pongono $W_0 \coloneqq 0$ e $W_i \coloneqq \langle w, Xw, \ldots, X^{i-1}w \rangle$, allora $XW_n = W_n$.

Sia $Y \in K$; per induzione, si mostra che $YW_{i+1} \subseteq W_{i+1}$. Infatti,

$$YX^i w = YXX^{i-1}w = XYX^{i-1}w - [X, Y]X^{i-1}w:$$

per il passo induttivo, $YX^{i-1}w \in W_i$ (da cui $XYX^{i-1}w \in W_{i+1}$) e $[X, Y]X^{i-1}w \in W_i$ (perché $[X, Y] \in K$). Ancora per induzione, si mostra che $YX^i w - \lambda(Y)X^i w \in W_i$: si considera la stessa formula di prima; per il passo induttivo, $YX^{i-1}w = \lambda(Y)X^{i-1}w + w'$, con $w' \in W_{i-1}$; d'altra parte $XW_{i-1} \subseteq W_i$ e $[X, Y]X^{i-1}w \in W_i$ perché $[X, Y] \in K$, quindi si ha l'asserto. I due risultati implicano che sulla base data dagli $X^i w$, Y è rappresentata da una matrice triangolare superiore con $\lambda(Y)$ sulla diagonale; in particolare $\mathrm{Tr}(Y_{|W_n}) = n\lambda(Y)$.

Si considera ora $[X, Y]$ con $X \in L$ e $Y \in K$; poiché K è un ideale, $[X, Y] \in K$ e quindi $\mathrm{Tr}([X, Y]_{|W_n}) = n\lambda([X, Y])$. Poiché $XW_n \subseteq W_n$ e $YW_n \subseteq W_n$, si ha che $[X, Y]_{|W_n}$ ha traccia nulla perché coincide con $[X_{|W_n}, Y_{|W_n}] = X_{|W_n}Y_{|W_n} - Y_{|W_n}X_{|W_n}$. In particolare, $\lambda([X, Y]) = 0$. □

Corollario 2.4.8. *Sia L una sottoalgebra risolubile di $\mathfrak{gl}(V)$, con V spazio vettoriale di dimensione finita su $\mathbb{C}$. Allora le matrici relative a L, in un'opportuna base, sono triangolari superiori, cioè L stabilizza una bandiera di sottospazi.*

Osservazione 2.4.9. Se L è un'algebra risolubile, e $\varphi\colon L \to \mathrm{End}(M)$ è una rappresentazione su uno spazio vettoriale M, allora il teorema si applica a $\varphi(L) \subseteq \mathrm{End}(M)$.

Il teorema si può anche applicare con la mappa $\mathrm{ad}\colon L \to \mathrm{Aut}(L)$, se L è risolubile. In particolare, un'algebra complessa risolubile ammette sempre una bandiera di ideali.

2.5 Il sistema di radici

Si considera un'algebra di Lie semisemplice reale $\mathfrak{g}$ di un gruppo compatto G. Si sa che $\mathfrak{g} = R_1 \oplus \cdots \oplus R_s$ con R_i ideali semplici. Sia $T \subseteq G$ un toro massimale; allora T_e è una sottoalgebra di Lie di $\mathfrak{g}$ abeliana che si chiama *sottoalgebra torale massimale* e soddisfa $\mathfrak{g} = T_e \oplus V_1 \oplus \cdots \oplus V_r$, dove i V_i sono spazi di dimensione 2 su cui un elemento $\exp(X) \in T$, con $X \in T_e$, agisce come $\begin{pmatrix} \cos(2\pi\vartheta_i(X)) & -\sin(2\pi\vartheta_i(X)) \\ \sin(2\pi\vartheta_i(X)) & \cos(2\pi\vartheta_i(X)) \end{pmatrix}$. Nel paragrafo 1.4 abbiamo chiamato i funzionali $\pm\vartheta_r$ "le radici" di G. Si studia la complessificata $L \coloneqq \mathfrak{g} \oplus i\mathfrak{g} = T_{e,\mathbb{C}} \oplus V_{1,\mathbb{C}} \oplus \cdots \oplus V_{r,\mathbb{C}}$, dove $T_{e,\mathbb{C}}$ è la complessificata di T_e e $V_{i,\mathbb{C}}$ di V_i. Si ha che $T_{e,\mathbb{C}}$ agisce su $V_{i,\mathbb{C}}$ attraverso la mappa aggiunta

con matrici del tipo $\mathrm{diag}(e^{2\pi i\vartheta_i(X)}, e^{-2\pi i\vartheta_i(X)})$, poiché essendo il toro abeliano, si possono diagonalizzare contemporaneamente le matrici delle azioni. Quindi $L = T_{e,\mathbb{C}} \oplus \bigoplus_{\alpha\in\Phi} L_\alpha$, dove $L_{\pm\alpha_i}$ è lo spazio di dimensione 1 corrispondente all'autovalore $\pm\alpha_i = e^{\pm 2\pi i\vartheta_i}$. In particolare, $V_{j,\mathbb{C}} = L_{\alpha_j} \oplus L_{-\alpha_j}$ e, presi $h \in T_{e,\mathbb{C}}$
08.05.2007 e $l \in L_\alpha$, si ottiene $[h, l] = \alpha(h)l$.

Lemma 2.5.1. *Si ha* $[L_\alpha, L_\beta] \subseteq L_{\alpha+\beta}$.

Dimostrazione. Siano $l_\alpha \in L_\alpha$, $l_\beta \in L_\beta$ e $h \in T_{e,\mathbb{C}}$; allora

$$\begin{aligned}[h,[l_\alpha,l_\beta]] &= -[l_\beta,[h,l_\alpha]] - [l_\alpha,[l_\beta,h]] = \alpha(h)[l_\alpha,l_\beta] + \beta(h)[l_\alpha,l_\beta] = \\ &= (\alpha(h)+\beta(h))[l_\alpha,l_\beta] = (\alpha+\beta)(h)[l_\alpha,l_\beta].\end{aligned}$$ □

Lemma 2.5.2. *Siano* $\alpha, \beta \in \Phi \cup \{0\}$ *tali che* $\alpha + \beta \neq 0$*, allora* $L_\alpha \perp L_\beta$ *rispetto alla forma di Killing.*

Dimostrazione. Siano l_α, l_β e h come nella dimostrazione del lemma 2.5.1, scegliendo però h in modo che $(\alpha+\beta)(h) \neq 0$; allora

$$\begin{aligned}\alpha(h)k(l_\alpha,l_\beta) &= k(\alpha(h)l_\alpha,l_\beta) = k([h,l_\alpha],l_\beta) = -k([l_\alpha,h],l_\beta) = \\ &= -k(l_\alpha,[h,l_\beta]) = k(l_\alpha,\beta(h)l_\beta) = -\beta(h)k(l_\alpha,l_\beta).\end{aligned}$$

Di conseguenza, $(\alpha+\beta)(h)k(l_\alpha,l_\beta) = 0$, ma $(\alpha+\beta)(h) \neq 0$, quindi deve essere $k(l_\alpha,l_\beta) = 0$. □

Proposizione 2.5.3. *La forma di Killing di* $\mathfrak{g}$ *estesa a* L *e ristretta a* $T_{e,\mathbb{C}}$ *è non degenere.*

Dimostrazione. La forma di Killing su $\mathfrak{g}$ è definita negativa, mentre su $i\mathfrak{g}$ è definita positiva. Di conseguenza è non degenere su tutto L; inoltre, $L_0 = T_{e,\mathbb{C}}$ è ortogonale a L_α per ogni $\alpha \in \Phi$. Se ora la forma di Killing fosse degenere su L_0, esisterebbe $h \in L_0$ tale che $k(h,h') = 0$ per ogni $h' \in L_0$, ma anche per ogni $h' \in L$ per l'ortogonalità, e questo è assurdo dato che k è non degenere su L. □

Osservazione 2.5.4. Grazie al fatto che la forma di Killing è non degenere su $T_{e,\mathbb{C}}$, si ha un'identificazione canonica con il duale: a $\varphi \in T^\star_{e,\mathbb{C}}$ si associa $t_\varphi \in T_{e,\mathbb{C}}$ tale che $k(t_\varphi, h) = \varphi(h)$.

Proposizione 2.5.5.
1. *Il duale di* $T_{e,\mathbb{C}}$ *è generato da* Φ*;*
2. *se* $\alpha \in \Phi$, $-\alpha \in \Phi$*;*
3. *se* $\alpha \in \Phi$, $x \in L_\alpha$ *e* $y \in L_{-\alpha}$*, allora* $[x,y] = k(x,y)t_\alpha$*;*
4. *se* $\alpha \in \Phi$*, allora* $\dim L_\alpha = 1$ *e* $[L_\alpha, L_{-\alpha}] = \langle t_\alpha\rangle$ *ha dimensione* 1*;*
5. $\alpha(t_\alpha) = k(t_\alpha,t_\alpha) \neq 0$*;*
6. *se* $\alpha \in \Phi$ *e* $x \in L_\alpha \setminus \{0\}$*, allora esiste* $y \in L_{-\alpha}$ *tale che* $\langle x, y, [x,y]\rangle \cong \mathfrak{sl}(2,\mathbb{C})$.

Dimostrazione.
1. Se Φ non generasse $T^\star_{e,\mathbb{C}}$, i t_α non genererebbero $T_{e,\mathbb{C}}$, perciò esisterebbe $h \neq 0$ tale che $0 = k(t_\alpha, h) = \alpha(h)$ per ogni $\alpha \in \Phi$, da cui $[h, l_\alpha] = \alpha(h)l_\alpha = 0$ per ogni $l_\alpha \in L_\alpha$ e $\alpha \in \Phi$; inoltre $[h, T_{e,\mathbb{C}}] = 0$ perché $T_{e,\mathbb{C}}$ è abeliana. Si è ottenuto che $h \in \mathrm{Z}(L)$, ma L è un'algebra semisemplice e in particolare $\mathrm{Z}(L) = 0$, assurdo.

2. Se $-\alpha$ non appartenesse a Φ, allora $k(L_\alpha, L) = 0$, perché L_α e L_β sarebbero ortogonali per ogni β, ma questo contraddirebbe il fatto che k è non degenere.

3. Per l'invarianza della forma di Killing, per ogni $x \in L_\alpha$ e $y \in L_{-\alpha}$, si ha
$$\begin{aligned} k(h, [x, y]) &= k([h, x], y) = \alpha(h)k(x, y) = k(t_\alpha, h)k(x, y) = \\ &= k(k(x, y)t_\alpha, h) = k(h, k(x, y)t_\alpha). \end{aligned}$$
Allora $k(h, [x, y] - k(x, y)t_\alpha) = 0$ per ogni $h \in T_{e,\mathbb{C}}$. Ma $[x, y] - k(x, y)t_\alpha \in T_{e,\mathbb{C}}$ e la forma è non degenere, perciò deve essere $[x, y] = k(x, y)t_\alpha$.

4. Si sa che $\dim L_\alpha = 1$ e, per il punto 3, che $[L_\alpha, L_{-\alpha}] \leq \langle t_\alpha \rangle$. Sia $x \in L_\alpha \setminus \{0\}$, allora se $k(x, L_{-\alpha}) = 0$, $k(x, L) = 0$, dato che per ogni altro β, $k(x, L_\beta) = 0$ per l'ortogonalità. Quindi dato che k è non degenere, deve essere $k(x, L_{-\alpha}) \neq 0$. Ma allora, sempre per il punto precedente, $[x, L_{-\alpha}] \neq 0$.

5. Per assurdo, sia $\alpha(t_\alpha) = 0$; allora per ogni $x \in L_\alpha$ e $y \in L_{-\alpha}$, si ha $[t_\alpha, x] = 0 = [t_\alpha, y]$. Si possono scegliere x e y in modo che $k(x, y) = 1$, cioè $[x, y] = t_\alpha$. Allora lo spazio $S \coloneqq \langle x, y, t_\alpha \rangle_{\mathbb{C}}$ è un'algebra risolubile, dato che i bracket definitivamente si annullano, e si ha $S \cong \mathrm{ad}(S) \subseteq \mathfrak{gl}(L)$, per l'iniettività della mappa aggiunta. Ora, da una parte $\mathrm{ad}(t_\alpha)$ è diagonalizzabile, in quanto t_α è elemento del toro; dall'altra, $\mathrm{ad}(t_\alpha) = \mathrm{ad}([x, y])$, che è nilpotente, dalla dimostrazione del teorema di Lie. Quindi $\mathrm{ad}(t_\alpha)$ deve essere nullo, ma ad è iniettiva, perciò $t_\alpha = 0$, assurdo.

6. Si sceglie $y \in L_{-\alpha}$ in modo che $k(x, y) = {}^2/_{k(t_\alpha, t_\alpha)}$ e si pone $h \coloneqq {}^{2t_\alpha}/_{k(t_\alpha, t_\alpha)}$. A questo punto si ha un isomorfismo dato da $x \mapsto e$, $y \mapsto f$, $h \mapsto h$, infatti si dimostra che $[x, y] = h$, $[h, x] = 2x$ e $[h, y] = -2y$. □

Proposizione 2.5.6. *Se $\alpha \in \Phi$, allora gli unici multipli di α che appartengono a Φ sono $\pm\alpha$.*

Dimostrazione. Sia $M \coloneqq T_{e,\mathbb{C}} \oplus \bigoplus_{c \in \mathbb{C}} L_{c\alpha} \subseteq L$; per il punto 6 della proposizione 2.5.5, si trovano $x \in L_\alpha$, $y \in L_{-\alpha}$ e $h \coloneqq [x, y] \in L_0$ tali che $\langle x, y, h \rangle \cong \mathfrak{sl}(2, \mathbb{C})$ agisce su M. Questa è una rappresentazione, che ha pesi 0 su $T_{e,\mathbb{C}}$ e $2c$ su $L_{c\alpha}$: infatti, poiché si è definito $h \coloneqq {}^{2t_\alpha}/_{k(t_\alpha, t_\alpha)}$:
$$[h, l_{c\alpha}] = c\alpha(h)l_{c\alpha} = k(t_\alpha, h)cl_{c\alpha} = 2\frac{k(t_\alpha, t_\alpha)}{k(t_\alpha, t_\alpha)}cl_{c\alpha} = 2cl_{c\alpha}.$$
Dato che i pesi sono interi, deve essere innanzitutto $c \in \mathbb{Z}[{}^1/_2]$.

Ora, posto $L' \coloneqq \bigoplus_{c \notin \{0, \pm 1\}} L_{c\alpha}$, $M = \ker(\alpha) \oplus \langle x, y, h \rangle \oplus L'$ e questa è una scomposizione in $\mathfrak{sl}(2, \mathbb{C})$-rappresentazioni: le prime due si calcolano, la terza si ottiene grazie al trucco unitario. Ma in L' non ci sono vettori di peso 0 per h, quindi non ci sono vettori di peso pari per h. Di conseguenza, 2α non è una radice, perché altrimenti, preso $l_{2\alpha} \in L_{2\alpha}$, si avrebbe $[h, l_{2\alpha}] = 4l_{2\alpha}$: $l_{2\alpha}$ avrebbe peso 4, assurdo.

Perciò neppure ${}^1/_2\alpha$ può essere radice, altrimenti $2\,{}^1/_2\alpha = \alpha$ non sarebbe radice; allora in M non c'è il peso 1 e per il corollario 2.3.10, $M = T_{e,\mathbb{C}} \oplus L_\alpha \oplus L_{-\alpha}$. □

Proposizione 2.5.7. 1. *Se $\alpha \in \Phi$, allora gli unici multipli di α in Φ sono α e $-\alpha$;*

2. *se $\alpha, \beta \in \Phi$ e $h_\alpha := {}^{2t_\alpha}/_{k(t_\alpha,\, t_\alpha)}$, allora $\beta(h_\alpha) \in \mathbb{Z}$ e $\beta - \beta(h_\alpha)\alpha \in \Phi$;*

3. *se $\alpha, \beta \in \Phi$ e $\alpha + \beta \in \Phi$, allora $[L_\alpha, L_\beta] = L_{\alpha+\beta}$;*

4. *se $\alpha, \beta \in \Phi$ e $\beta \neq \pm\alpha$, siano r e q i naturali massimali per cui $\beta - r\alpha \in \Phi$ e $\beta + q\alpha \in \Phi$, allora per ogni i, $r \leq i \leq q$, $\beta + i\alpha \in \Phi$ e inoltre $\beta(h_\alpha) = r - q$;*

5. *L è generata come algebra di Lie dagli L_α per $\alpha \in \Phi$.*

10.05.2007

Dimostrazione. Il primo punto è la proposizione 2.5.6.

Per il secondo e il quarto, sia $K := \sum_{l \in \mathbb{Z}} L_{\beta + l\alpha}$; K è un $\mathfrak{sl}(2, \mathbb{C})$-modulo, dove $\mathfrak{sl}(2, \mathbb{C})$ è la copia generata da L_α, $L_{-\alpha}$ e $\langle t_\alpha \rangle$. Si ha infatti, per $z \in L_{\beta+l\alpha}$, $[x_\alpha, z] \in L_{\alpha+(\beta+l\alpha)} \subseteq K$ e $[y_\alpha, z] \in L_{-a+(\beta+l\alpha)} \subseteq K$, mentre

$$[h_\alpha, z] = (\beta(h_\alpha) + l\alpha(h_\alpha))z = (\beta(h_\alpha) + 2\frac{k(t_\alpha, t_\alpha)}{k(t_\alpha, t_\alpha)} l)z = (\beta(h_\alpha) + 2l)z;$$

per quest'ultima, K è irriducibile, dato che $\dim L_0 + \dim L_1 = 1$. Essendo un $\mathfrak{sl}(2, \mathbb{C})$-modulo irriducibile, per il teorema di struttura delle $\mathfrak{sl}(2, \mathbb{C})$-rappresentazioni, K avrà un elemento di peso più alto, per $l = q$, e un elemento di peso minimo, per $l = -r$, e uno qualunque dei pesi intermedi deve appartenere a K. Inoltre, il peso massimo è l'opposto del peso minimo, cioè $(\beta + q\alpha)(h_\alpha) = -(\beta - r\alpha)(h_\alpha)$, da cui $2\beta(h_\alpha) = 2r - 2q$, ovvero $\beta(h_\alpha) = r - q \in \mathbb{Z}$.

Per il terzo punto, se $\alpha + \beta$ è una radice, allora $L_{\alpha+\beta} \neq \{0\}$, perciò $q \geq 1$. D'altra parte, per il teorema di struttura, applicando x_α a un vettore di L_β (di peso $\beta(h_\alpha)$), si ottiene un vettore di $L_{\beta+\alpha}$ di peso $\beta(h_\alpha) + 2$, che in particolare sarà non nullo. Allora $0 \neq [L_\alpha, L_\beta] \subseteq L_{\alpha+\beta}$, da cui si ha l'uguaglianza per questioni di dimensione.

Per il quinto punto, un elemento di L_α è ovviamente generato dagli L_α, così come i t_α sono generati dagli L_α; l'unica possibilità è che ci sia $h \in T_{e,\mathbb{C}}$ tale che $h \notin \langle t_\alpha \rangle$ per ogni $\alpha \in \Phi$, ma allora $[h, l_\alpha] = \alpha(h) l_\alpha = k(t_\alpha, h) l_\alpha = 0$, cioè $h \in \mathrm{Z}(L) = \{0\}$. □

Si sa che $\Phi \subseteq T^\star_{e,\mathbb{C}}$. Grazie alla forma di Killing si può dare un prodotto scalare $(\gamma, \delta) := k(t_\gamma, t_\delta)$ su $T_{e,\mathbb{C}}$. Si può rivisitare la proposizione: per esempio, si traduce $\beta(h_\alpha) = \beta({}^{2t_\alpha}/_{k(t_\alpha,\, t_\alpha)}) = {}^{2k(t_\beta,\, t_\alpha)}/_{k(t_\alpha,\, t_\alpha)}$ in ${}^{2(\beta,\, \alpha)}/_{(\alpha,\, \alpha)} \in \mathbb{Z}$, che è la proprietà di integralità richiesta a un sistema di radici. Ancora, $\beta - \beta(h_\alpha)\alpha \in \Phi$, $\beta - {}^{2(\beta,\, \alpha)}/_{(\alpha,\, \alpha)}\alpha \in \Phi$ è la simmetria rispetto all'iperpiano ortogonale a α.

Per completare l'identificazione delle radici di un'algebra di Lie con un sistema di radici, si può dimostrare che se $\alpha, \beta \in \Phi$, allora $(\alpha, \beta) \in \mathbb{Q}$. Questo permette di definire il prodotto scalare su $\langle \Phi \rangle_\mathbb{Q} \otimes_\mathbb{Q} \mathbb{R}$, che è lo spazio euclideo dove si costruisce il sistema di radici dopo l'identificazione.

2.6 Teorema di Poincaré-Birkhoff-Witt

Definizione 2.6.1. Siano K un campo e V uno spazio vettoriale su K; si pongono $T^0 V := K$, $T^1 V := V$, $T^n V := \bigotimes_{i=1}^n V$; da questi si costruisce l'*algebra tensoriale* di V, $\mathscr{T}(V) := \bigoplus_{i \geq 0} T^i V$.

L'algebra tensoriale è un'algebra associativa graduata con unità, non commutativa. È universale rispetto alla proprietà che data $\gamma\colon V \to A$ lineare, con A algebra associativa con unità, allora esiste $\tilde{\gamma}$ che fa commutare il diagramma:

$$\begin{tikzcd} V \arrow[rr, "\gamma"] \arrow[dr] & & A \\ & \mathscr{T}(V). \arrow[ur, dashed, "\tilde{\gamma}"'] & \end{tikzcd}$$

L'ideale $I \coloneqq (x \otimes y - y \otimes x)_{x,y \in L}$ è bilatero e si definisce $S(V) \coloneqq {}^{\mathscr{T}(V)}/_{I}$, l'*algebra simmetrica* su V. Quello che si ottiene è ancora un'algebra graduata, perché I è omogeneo, cioè $I = \bigoplus_{i \geq 2} I \cap T^i(V)$. È ancora universale, secondo la stessa proprietà, richiedendo però che A sia un'algebra associativa commutativa con unità. In particolare, $S(V)$ è isomorfa all'algebra dei polinomi $K[x_1, \dots, x_{\dim V}]$ (se $\dim V < \infty$), o all'algebra dei polinomi in infinite variabili.

Definizione 2.6.2. Data un'algebra di Lie L, l'*algebra inviluppante* di L è data da una coppia $(\mathscr{U}, i)$ dove:

1. $\mathscr{U}$ è un'algebra associativa con unità;
2. $i\colon L \to \mathscr{U}$ è lineare e $i([x,y]) = i(x)i(y) - i(y)i(x)$;
3. $\mathscr{U}$ è universale rispetto al diagramma seguente, dove A è un'algebra associativa con unità e j è lineare e tale che $j([x,y]) = j(x)j(y) - j(y)j(x)$:

$$\begin{tikzcd} L \arrow[rr, "j"] \arrow[dr, "i"'] & & A \\ & \mathscr{U}. \arrow[ur, dashed, "\tilde{j}"'] & \end{tikzcd}$$

Grazie alla proprietà universale, se esiste, l'algebra inviluppante è unica a meno di isomorfismi. Per l'esistenza, si costruisce esplicitamente l'algebra $\mathscr{U}(L) : = {}^{\mathscr{T}(L)}/_{J}$, dove J è l'ideale (non omogeneo) $(x \otimes y - y \otimes x - [x,y])_{x,y \in L}$. Si verifica senza troppe difficoltà che questa è davvero un'algebra inviluppante per L: data $j\colon L \to A$, è sufficiente definire j' come j sugli elementi di grado 1, estenderla nel modo ovvio a $\mathscr{T}(L)$ e verificare che passa al quoziente.

Il fatto che l'ideale J non sia omogeneo crea dei problemi: per esempio, dato che il quoziente coinvolge elementi di grado 1, non è banale sapere se si può immergere L in ${}^{\mathscr{T}(L)}/_{J}$; però, dato che $J \cap T^0 L = \{0\}$, si sa che la proiezione $\pi\colon \mathscr{T}(L) \to {}^{\mathscr{T}(L)}/_{J}$ è iniettiva su $T^0 L$.

Esempio 2.6.3. Se L è abeliana, allora $\mathscr{U}(L) = S(L)$, dato che l'ideale J si riduce a I.

Esempio 2.6.4. Si considera $\mathfrak{sl}(2, \mathbb{C})$; una base è data da h, f, e. I polinomi ordinati $h^a f^b e^c$ formano una base di $\mathscr{U}(\mathfrak{sl}(2,\mathbb{C}))$, poiché grazie alle relazioni (in $\mathscr{U}(\mathfrak{sl}(2,\mathbb{C}))$)

$$\begin{aligned} h &= [e,f] = e \otimes f - f \otimes e, \\ 2e &= [h,e] = h \otimes e - e \otimes h, \\ -2f &= [h,f] = h \otimes f - f \otimes h, \end{aligned}$$

ogni elemento di $\mathscr{U}(\mathfrak{sl}(2,\mathbb{C}))$ si può ordinare, portando all'inizio i termini in h e alla fine i termini in e.

Sottointendendo lo spazio vettoriale, sia $T_m \coloneqq T^0 \oplus T^1 \oplus \cdots \oplus T^m$; allora $T_0 \subseteq \cdots T_m \subseteq \cdots$ è una filtrazione di T. Sia $\mathscr{U}_m \coloneqq \pi(T_m)$, le proiezioni di T_m in $\mathscr{U}$. Ponendo $\mathscr{U}_{-1} \coloneqq \{0\}$, si ha che $\mathscr{U}_{-1} \subseteq \cdots \subseteq \mathscr{U}_m \subseteq \cdots$ è una filtrazione di $\mathscr{U}$ e inoltre $\mathscr{U}_m\mathscr{U}_p \subseteq \mathscr{U}_{m+p}$.

Definizione 2.6.5. Ponendo $G^m \coloneqq {}^{\mathscr{U}_m}/_{\mathscr{U}_{m-1}}$ (con la moltiplicazione indotta da quella di $\mathscr{U}$, che si dimostra essere ben definita), si definisce l'*algebra graduata associata alla filtrazione* $\mathscr{U}_m$ come $\mathscr{G} \coloneqq \bigoplus_{m\geq 0} G^m$. In particolare, $\mathscr{G}$ è un'algebra graduata associativa con unità.

Si può definire la mappa $\varphi_m\colon T^m \xrightarrow{\pi} \mathscr{U}_m \to G^m$; φ_m è suriettiva, perché la proiezione degli m-tensori è proprio ciò che differenzia $\mathscr{U}_m$ da $\mathscr{U}_{m-1}$. Considerando tutte le φ_m si ha una mappa $\varphi\colon \mathscr{T} \to \mathscr{G}$ lineare e suriettiva, anche se non è detto che sia una mappa di algebre.

Lemma 2.6.6. *La mappa $\varphi\colon \mathscr{T} \to \mathscr{G}$ è morfismo di algebre. Inoltre $\varphi(I) = 0$, dunque φ induce un morfismo di algebre suriettivo $\omega\colon S \to \mathscr{G}$. In particolare $\mathscr{G}$ è commutativo.*

Dimostrazione. È un morfismo di algebre per la definizione del prodotto su $\mathscr{G}$; $\varphi(I) = 0$ perché, in $\mathscr{U}$, $x \otimes y$ e $y \otimes x$ differiscono di elementi di grado inferiore, che vengono annullati dal quoziente. $\square$

Teorema 2.6.7 (Poincaré-Birkhoff-Witt)**.** *Il morfismo ω è un isomorfismo di algebre.*

Corollario 2.6.8. *Sia:*

$$\begin{tikzcd} T^m \arrow[r, "\pi"] \arrow[d] & \mathscr{U}_m \arrow[d] \\ S^m \arrow[r, "\omega"'] & G^m. \end{tikzcd}$$

Se $W \leq T^m$ è un sottospazio che viene mandato isomorficamente su S^m, allora $\pi(W)$ è un complementare di $\mathscr{U}_{m-1}$ in $\mathscr{U}_m$.

Dimostrazione. Per il teorema, W viene mandato isomorficamente in G^m attraverso S^m, allora deve essere mandato isomorficamente in G^m anche attraverso $\mathscr{U}_m$. Di conseguenza, $\pi(W) \oplus \mathscr{U}_{m-1} = \mathscr{U}_m$. $\square$

Corollario 2.6.9. *Si ottiene che $L \oplus \mathscr{U}_0 = \mathscr{U}_1$ e che $\pi_{|L}$ è iniettiva. In particolare, si può mappare l'algebra di Lie L dentro la sua algebra inviluppante.*

Dimostrazione. Considerando lo stesso diagramma del corollario 2.6.8 per $m = 1$, prendendo $W = L = T^1$, si ha un isomorfismo di W su S^1 (perché $S = {}^{\mathscr{T}}/_{I}$ con I che non coinvolge termini di primo grado) e quindi $L \oplus \mathscr{U}_0 = \mathscr{U}_1$ e $\pi_{|L}$ è iniettiva. $\square$

15.05.2007 **Corollario 2.6.10.** *Sia $(x_1, \ldots, x_n, \ldots)$ una base di L; allora gli elementi $x_{i(1)} \cdots x_{i(m)} = \pi(x_{i(1)} \otimes \cdots \otimes x_{i(m)})$ dove $m \in \mathbb{Z}^+$ e $i(1) \leq i(2) \leq \cdots \leq i(m)$, insieme a 1, sono una base di $\mathscr{U}$.*

Dimostrazione. Segue dal corollario 2.6.8, trovando la base grado per grado. $\square$

Dimostrazione del teorema di Poincaré-Birkhoff-Witt. Si fissa una base ordinata $(x_\lambda)_{\lambda\in\Lambda}$ di L; si identifica S con l'algebra dei polinomi nelle x_λ (denotando le variabili con z_λ per distinguerle). Se $\Sigma = (\lambda_1, \dots, \lambda_m)$ è una lista di indici, allora:

1. si dice che Σ ha *lunghezza* m;
2. si pongono $z_\Sigma \coloneqq z_{\lambda_1} \cdots z_{\lambda_m}$ e $x_\Sigma \coloneqq x_{\lambda_1} \otimes \cdots \otimes x_{\lambda_m}$;
3. se $\lambda_1 \le \cdots \le \lambda_m$, si dice che Σ è *crescente*;
4. se $\lambda \le \lambda_i$ per ogni i, si scrive $\lambda \le \Sigma$;
5. per convenzione, si dice che $\varnothing$ è una lista crescente e si definisce $z_\varnothing = 1$.

Con queste notazioni, una base di S è data da tutti gli z_Σ con Σ crescente.

Lemma 2.6.11. *Per ogni $m \in \mathbb{Z}^+$, esiste un'unica mappa lineare $f_m \colon L\otimes S_m \to S$ (con $S_m \coloneqq S^0 \oplus \cdots \oplus S^m$, la filtrazione associata alla gradazione su S) tale che:*

1. $f_m(x_\lambda \otimes z_\Sigma) = z_\lambda z_\Sigma$ *se* $\lambda \le \Sigma$ *e* $z_\Sigma \in S_m$*;*
2. $f_m(x_\lambda \otimes z_\Sigma) = z_\lambda z_\Sigma \pmod{S_k}$ *se* $k \le m$ *e* $z_\Sigma \in S_k$*;*
3. $f_m(x_\lambda \otimes f_m(x_\eta \otimes z_\mathrm{T})) = f_m(x_\eta \otimes f_m(x_\lambda \otimes z_\mathrm{T})) + f_m([x_\lambda, x_\eta] \otimes z_\mathrm{T})$ *se* $z_\mathrm{T} \in S_{m-1}$.

Inoltre, f_m coincide con f_{m-1} su $L \otimes S_{m-1}$.

Dimostrazione. Si osserva innanzitutto che il terzo punto ha senso grazie al secondo, per cui $f_m(x_\eta \otimes z_\mathrm{T}) \in S_m$. Inoltre se f_m con le tre proprietà esiste ed è unica, necessariamente si ha l'ultima osservazione di coincidenza con f_{m-1}.

Per induzione su m si mostra che f_m esiste ed è unica. Per $m = 0$, le richieste si riducono a $f_0(x_\lambda \otimes 1) = z_\lambda$, quindi non c'è nessun problema. Si suppone ora di avere f_{m-1} che soddisfa le proprietà e di volerla estendere a f_m.

Presa una lista ordinata Σ di lunghezza m, va definito $f_m(x_\lambda\otimes z_\Sigma)$; se $\lambda \le \Sigma$, per la prima proprietà si deve porre $f_m(x_\lambda\otimes z_\Sigma) \coloneqq z_\lambda z_\Sigma$. Se invece $\lambda \not\le \Sigma$, posto $\Sigma = (\mu, T)$ con $\mu < \lambda$, si sa che $f_{m-1}(x_\mu \otimes z_\mathrm{T}) = z_\mu z_\mathrm{T}$ per induzione; allora

$$f_m(x_\lambda\otimes z_\Sigma) = f_m(x_\lambda\otimes z_\mu z_\mathrm{T}) = f_m(x_\lambda\otimes f_{m-1}(x_\mu\otimes z_\mathrm{T})) = f_m(x_\lambda\otimes f_m(x_\mu\otimes z_\mathrm{T}))$$

e si è obbligati a deve definire f_m come il secondo membro della terza proprietà, che però è espresso ancora in termini di f_m: cioè si pone

$$f_m(x_\lambda \otimes z_\Sigma) \coloneqq f_m(x_\mu \otimes f_m(x_\lambda \otimes z_T)) + f_m([x_\lambda, x_\mu] \otimes z_T).$$

Per la seconda, $f_m(x_\lambda \otimes z_\mathrm{T}) = f_{m-1}(x_\lambda \otimes z_\mathrm{T}) = z_\lambda z_\Sigma + y$, con $y \in S_{m-1}$. Con questa osservazione, si mostra che l'espressione che sembrava dipendere ancora da f_m in realtà è già completamente definita: il primo addendo si trasforma in

$$f_m(x_\mu \otimes z_\lambda z_\mathrm{T}) + f_m(x_\mu \otimes y) = z_\mu z_\lambda z_\mathrm{T} + f_{m-1}(x_\mu \otimes y)$$

rispettivamente per la prima proprietà (dato che $\mu \le (\lambda, \mathrm{T})$) e perché $y \in S_{m-1}$; il secondo addendo è $f_{m-1}([x_\lambda, x_\mu] \otimes z_\mathrm{T})$, ancora perché $z_\mathrm{T} \in S_{m-1}$. Si è dimostrato che la f_m può essere definita e le proprietà implicano l'unicità.

L'ultima cosa da dimostrare è che f_m così definita soddisfa le tre relazioni. La prima è soddisfatta per costruzione; per la seconda, scelto $k \leq m$ e z_Σ con $\Sigma = (\mu, T)$ di lunghezza k, se $\lambda \leq \mu$ si conclude subito per il primo punto, altrimenti si ha

$$\begin{aligned} f_m(x_\lambda \otimes z_\Sigma) = f_k(x_\lambda \otimes z_\Sigma) &= f_k(x_\lambda \otimes f_k(x_\mu \otimes z_\mathrm{T})) = \\ &= z_\mu z_\lambda z_\mathrm{T} + f_{k-1}(x_\lambda \otimes y) + f_{k-1}([x_\lambda, x_\mu] \otimes z_\mathrm{T}) \end{aligned}$$

e gli ultimi due addendi appartengono a S_k. La terza vale per costruzione quando $\eta < \lambda$ e $\eta \leq \mathrm{T}$; se $\lambda = \eta$ la condizione non dice nulla, perché $[x_\lambda, x_\eta] = 0$; se nella proprietà si scambiano λ con η si ottiene la stessa condizione, quindi vale anche per $\lambda < \eta$ e $\lambda \leq \mathrm{T}$. Rimane da verificare quando né λ né η sono minori o uguali a T. Sia quindi $\mathrm{T} = (\mu, \Psi)$ di lunghezza $m - 1$ con $\mu < \lambda$ e $\mu < \eta$; si abbrevia $f_m(x \otimes z)$ con xz. Per la terza proprietà applicata al grado $m - 1$,

$$x_\eta z_\mathrm{T} = x_\eta(x_\mu z_\Psi) = x_\mu(x_\eta z_\Psi) + [x_\eta, x_\mu] z_\Psi,$$

mentre per la seconda, sempre in grado $m - 1$, si ha $x_\eta z_\Psi = z_\eta z_\Psi + w$, con $w \in S_{m-2}$. Per $x_\lambda(x_\mu(z_\eta z_\Psi))$ e per $x_\lambda(x_\mu w)$, la terza proprietà è già stata dimostrata, rispettivamente perché $\mu < \eta$ e per induzione (w ha grado $m - 2$), quindi vale anche per la loro somma, che sostituendo equivale a $x_\lambda(x_\mu(x_\eta z_\Psi))$:

$$x_\lambda(x_\mu(z_\eta z_\Psi + w)) = x_\lambda(x_\mu(x_\eta z_\Psi)) = x_\mu(x_\lambda(x_\eta z_\Psi)) + [x_\lambda, x_\mu](x_\eta z_\Psi).$$

Infine, applicando x_λ alla prima equazione trovata e usando due volte la terza proprietà, si ottiene

$$\begin{aligned} x_\lambda(x_\eta z_\mathrm{T}) &= x_\lambda(x_\mu(x_\eta z_\Psi)) + x_\lambda([x_\eta, x_\mu] z_\Psi) = \\ &= x_\mu(x_\lambda(x_\eta z_\Psi)) + [x_\lambda, x_\mu](x_\eta z_\Psi) + [x_\eta, x_\mu](x_\lambda z_\Psi) + [x_\lambda, [x_\eta, x_\mu]] z_\Psi. \end{aligned}$$

Se si ripete scambiando λ e η e si sottrae, applicando Jacobi rimane solo $x_\lambda(x_\eta z_\mathrm{T}) - x_\eta(x_\lambda z_\mathrm{T}) = [x_\lambda, x_\eta] z_\mathrm{T}$, la proprietà richiesta. □

Lemma 2.6.12. *Esiste una rappresentazione* $\rho \colon L \to \mathrm{End}(S)$ *tale che* $\rho(x_\lambda) z_\Sigma = z_\lambda z_\Sigma$ *se* $\lambda \leq \Sigma$ *e* $\rho(x_\lambda) z_\Sigma = z_\lambda z_\Sigma \pmod{S_m}$ *se* Σ *ha lunghezza* m.

Dimostrazione. La mappa f_m del lemma 2.6.11 è costruita a ogni grado in modo da essere compatibile con quelle definite nei gradi inferiori, quindi esiste una mappa $f \colon L \otimes S \to S$ tale che per $x_\lambda \in L$ e $z_\Sigma \in S_m$, $f(x \otimes z_\Sigma) := f_m(x \otimes z_\Sigma)$; f si può vedere come una rappresentazione di L. Le formule dicono come agisce x_λ su S: in particolare per S_m, ponendo $\rho(x_\lambda)(z_\Sigma) := f(x_\lambda \otimes z_\Sigma)$, si ha che $[\rho(x_\lambda), \rho(x_\mu)] z_\mathrm{T} = \rho(x_\lambda)\rho(x_\mu) z_\mathrm{T} - \rho(x_\mu)\rho(x_\lambda) z_\mathrm{T} = \rho([x_\lambda, x_\mu]) z_\mathrm{T}$. □

Lemma 2.6.13. *Sia* $t \in T_m \cap J$*; allora la componente omogenea* t_m *di grado* m *di* t *appartiene a* I.

Dimostrazione. Si scrive: $t_m = \sum \gamma_i x_{\Sigma(i)}$, con $\Sigma(i)$ liste di indici di lunghezza m. Per la proprietà universale di $\mathscr{T}$, il morfismo $\rho \colon L \to \mathrm{End}(S)$ si estende a un altro morfismo, chiamato ρ', da $\mathscr{T}$ a $\mathrm{End}(S)$. Poiché ρ soddisfa $[\rho(x), \rho(y)] = \rho([x, y])$ (essendo un morfismo di algebre di Lie dal lemma 2.6.12), ρ' si fattorizza per J, cioè $J \subseteq \ker(\rho')$, infatti

$$\rho'(x \otimes y - y \otimes x - [x, y]) = \rho'(x)\rho'(y) - \rho'(y)\rho'(x) - \rho'(x)\rho'(y) + \rho'(y)\rho'(x) = 0;$$

allora si può definire $\tilde{\rho}\colon \mathscr{U} = \mathscr{T}/J \to \mathrm{End}(S)$.

Tornando a t, $\rho'(t) = 0$ perché $t \in J \subseteq \ker(\rho')$; ma $\rho(t)(1) \in S$ è un polinomio il cui termine di grado più alto è $\sum \gamma_i z_{\Sigma(i)}$, per il lemma 2.6.11, perciò dovrà essere $\sum \gamma_i z_{\Sigma(i)} = 0$ in S. Dunque t_m viene mandato in 0 dalla mappa $\mathscr{T} \to S = \mathscr{T}/I$, cioè $t_m \in I$. □

Ora si può concludere il teorema, mostrando l'iniettività di ω (si è già dimostrata la suriettività nel lemma 2.6.6): sia $t \in T^m$ con $\pi(t) \in \ker(\omega)$, cioè tale che $\varphi(t) = 0$; si deve dimostrare che $t = 0$ in S, cioè che $t \in I$. Questo è sufficiente perché φ manda T^m in G^m, quindi basta prendere un t omogeneo.

Poiché t viene mandato in 0 da φ, $\pi(t) \in \mathscr{U}_{m-1}$, su cui si mappa suriettivamente T_{m-1}. Di conseguenza, deve esistere $t' \in T_{m-1}$ tale che $\pi(t') = \pi(t)$; allora $t - t' \in T_m$ e $t - t' \in J$, perché $\pi(t - t')$ è nullo in $\mathscr{U} = \mathscr{T}/J$. Per il lemma 2.6.13, la componente di grado m di $t - t'$ appartiene a I, ma t' ha componenti di grado al più $m - 1$ e t ha solo la componente di grado m, perciò si ha $t \in I$. □

2.7 Teoria delle rappresentazioni delle algebre di Lie semisemplici complesse

17.05.2007

Si sono affrontate in precedenza le algebre del tipo $L = \mathfrak{g} \oplus i\mathfrak{g}$, con $\mathfrak{g}$ compatta semisemplice reale. Un'algebra di questo tipo si spezza come $L = T_{e,\mathbb{C}} \oplus \bigoplus_{\alpha\in\Phi} L_\alpha$, dove Φ sono le radici. Sia V un L-modulo di dimensione finita; si è già visto che gli elementi $h \in T_{e,\mathbb{C}}$ agiscono su V con matrici diagonalizzabili. Infatti, $T_{e,\mathbb{C}} = \langle\, h_{\alpha_i} \mid \alpha \in \Delta \,\rangle$, dove Δ è una base del sistema di radici; h_{α_i} appartiene a $\langle x_{\alpha_i}, y_{\alpha_i}, h_{\alpha_i} \rangle \cong \mathfrak{sl}(2, \mathbb{C})$; V, in quanto $\mathfrak{sl}(2, \mathbb{C})$-modulo, si spezza in sottomoduli irriducibili, su ognuno dei quali h_{a_i} agisce in modo diagonale; infine, gli h_{α_i} commutano tra loro, per cui sono diagonalizzabili simultaneamente.

Definizione 2.7.1. Sia $V_\lambda \coloneqq \{\, w \in V \mid (\forall h \in T_{e,\mathbb{C}}) hw = \lambda(h)w \,\}$ con $\lambda \in T^\star_{e,\mathbb{C}}$; si dice che V_λ è lo *spazio peso* relativo al peso λ.

Grazie alle considerazioni fatte sulla simultanea diagonalizzabilità, si ha la seguente.

Proposizione 2.7.2. *Se V è un L-modulo di dimensione finita, allora $V = \bigoplus_{\lambda\in T^\star_{e,\mathbb{C}}} V_\lambda$.*

La somma è fatta solo su un numero finito di λ, gli altri danno $V_\lambda = 0$. Una situazione simile si ha quando si faceva agire $T_{e,\mathbb{C}}$ su L stesso.

Se V non è di dimensione finita, si possono ancora definire i V_λ, ma non è più vero che $\sum V_\lambda = V$: sia V' tale somma, che si mostra essere diretta. Come per le rappresentazioni di $\mathfrak{sl}(2, \mathbb{C})$, si scoprirà che esiste uno spazio peso di peso massimale, rispetto alla relazione $\lambda > \mu$ se e solo se $\lambda - \mu$ è una combinazione lineare a coefficienti positivi di radici semplici. Allora, ponendo $\Phi^+ \coloneqq \{\, \lambda \in \Phi \mid \lambda > 0 \,\}$ e presa $\alpha \in \Phi^+$, $[L_\alpha, V_\lambda]$ dovrebbe avere peso $\lambda + \alpha$, quindi $[L_\alpha, V_\lambda] = 0$. Lo spazio peso di peso massimale sarà caratterizzato dalla proprietà $\lambda(\alpha_i) \in \mathbb{N}$ per ogni $\alpha_i \in \Delta$.

Definizione 2.7.3. Un *vettore massimale* v^+ di un L-modulo V, è un vettore non nullo tale che $L_\alpha v^+ = 0$ per ogni $\alpha \in \Phi^+$.

Esempio 2.7.4. Si considera $\mathfrak{sl}(4,\mathbb{C})$ che agisce su se stessa tramite l'azione aggiunta; uno spezzamento naturale è quello in cui $T_{e,\mathbb{C}}$ è costituito dalle matrici diagonali e L_{α_1}, L_{α_2}, L_{α_3} da quelle non nulle su un elemento della sopradiagonale. Un elemento dell'algebra annullato via bracket dalle matrici triangolari superiori è $L_{\alpha_1+\alpha_2+\alpha_3}$, quello associato all'elemento più in alto a destra, ed è anche l'unico (a meno di scalari). Si verifica facilmente che questo dipende fortemente dalla base scelta. Un algoritmo utile per trovare nuove basi consiste nell'aggiungere al diagramma di Dynkin, che in questo caso è A_3, la radice $-(\alpha_1+\alpha_2+\alpha_3)$, aggiungendo a loro volta gli archi dalla nuova radice a α_1 e α_3 (perché $\langle \alpha_1, -(\alpha_1+\alpha_2+\alpha_3)\rangle = 1$ e così via); successivamente si può cancellare uno qualsiasi degli altri vertici del diagramma.

Definizione 2.7.5. Scelta una base Δ di Φ e spezzata L di conseguenza, la *sottoalgebra di Borel* è $B(\Delta) \coloneqq T_{e,\mathbb{C}} \oplus \bigoplus_{\alpha\in\Phi^+} L_\alpha$.

Essere un vettore massimale significa essere un vettore che viene annullato da tutta la parte strettamente positiva della sottoalgebra di Borel. Data una rappresentazione V e una base Δ, ci si può chiedere se esiste un vettore massimale in V; deve essere annullato da tutta la parte positiva di $B(\Delta)$, cioè $[B(\Delta), B(\Delta)] = \bigoplus_{\alpha\in\Phi^+} L_\alpha$. Si osserva che $B(\Delta)$ contiene gli spazi relativi alle radici di altezza (dove con altezza si intende la somma dei coefficienti nella scrittura rispetto a Δ) maggiore o uguale a 0; proseguendo ulteriormente con i bracket, si ottengono spazi relativi a radici di altezza sempre maggiore, che prima o poi termineranno, cioè $B(\Delta)$ è risolubile. Se $\dim V < \infty$, esiste un vettore in V annullato da tutta la parte positiva di $B(\Delta)$, cioè un vettore massimale; infatti $[L_\alpha, V_\lambda] \subseteq V_{\lambda+\alpha}$, da cui si ha che le matrici relative a elementi della parte positiva hanno la diagonale nulla; unito al corollario 2.4.8 al teorema di Lie, si ha che le matrici delle azioni sono strettamente triangolari superiori. Se invece la dimensione è infinita, non è detto che un vettore massimale esista.

Definizione 2.7.6. Un L-modulo è detto *ciclico standard di peso massimale* λ se è della forma $\mathscr{U}(L)v^+$, con v^+ un vettore massimale di peso λ.

Teorema 2.7.7. *Sia V un L-modulo ciclico standard con v^+ vettore massimale di peso λ; sia $\Phi^+ = \{\beta_1, \dots, \beta_m\}$, allora:*

1. *V è generato dai vettori $y_{\beta_1}^{i_1} \cdots y_{\beta_m}^{i_m} v^+$ con $i_j \in \mathbb{N}$; in particolare V è la somma diretta dei suoi spazi peso (cioè $V = V'$);*
2. *i pesi di V sono della forma $\mu = \lambda - \sum_{\alpha_i\in\Delta} k_i\alpha_i$ con $k_i \in \mathbb{N}$;*
3. *gli spazi peso V_μ hanno dimensione finita e V_λ ha dimensione 1;*
4. *ogni sottomodulo di V è somma diretta di spazi peso;*
5. *V è indecomponibile con un unico sottomodulo proprio massimale e quindi con un unico quoziente irriducibile.*

Dimostrazione. 1. È una conseguenza di Poincaré-Birkhoff-Witt: preso un elemento di $\mathscr{U}(L)$, si può ordinare, mettendolo nella forma $y_{\beta_1}^{i_1} \cdots y_{\beta_m}^{i_m} h_{\beta_1}^{j_1} \cdots h_{\beta_m}^{j_m} x_{\beta_1}^{k_1} \cdots x_{\beta_m}^{k_m}$; agendo su v^+, gli x lo annullano, quindi non devono essere presenti; gli h mandano v^+ in un suo multiplo, perché $v^+ \in V_\lambda$, quindi per generare V bastano gli elementi del tipo $y_{\beta_1}^{i_1} \cdots y_{\beta_m}^{i_m}$.

2. Il vettore $v := y_{\beta_1}^{i_1} \cdots y_{\beta_m}^{i_m} v^+$ ha peso $\lambda - \sum i_j \beta_j$ applicando ripetutamente
$$hy_{\beta_i} v^+ = [h, y_{\beta_i}]v^+ + y_{\beta_i} hv^+ = -\beta_i(h) y_{\beta_i} v^+ + \lambda(h) y_{\beta_i} v^+.$$

3. Le combinazioni che generano un certo peso, sono obbligatoriamente in numero finito per il punto precedente; in particolare, per avere il peso λ non si può applicare alcun y_{β_i}.

4. Preso Γ un sottomodulo di V, si deve dimostrare che $\Gamma = \bigoplus_\mu \Gamma \cap V_\mu$. Siano $w \in \Gamma$ e $w = v_1 + \cdots + v_n$ una scrittura minima rispetto a n tale che $v_i \in V_{\mu_i} \setminus \Gamma$; si sceglie h tale che $\mu_1(h) \neq \mu_2(h)$. Allora $hw = \mu_1(h)v_1 + \cdots + \mu_n(h)v_n \in \Gamma$, ma anche $\mu_1(h)w \in \Gamma$; sottraendo si ottiene che $(\mu_2(h) - \mu_1(h))v_2 + \cdots + (\mu_n(h) - \mu_1(h))(v_n) \in \Gamma$, che viola la minimalità.

5. Ogni sottomodulo proprio di V è somma di spazi peso e non può contenere V_λ (altrimenti sarebbe uguale a V); ne segue che la somma di tutti questi sottomoduli è ancora propria; la somma sarà l'unico sottomodulo massimale di V, che corrisponde a un unico quoziente irriducibile. □

Teorema 2.7.8. *Per ogni $\lambda \in T_{e,\mathbb{C}}^\star$, esiste un unico modulo ciclico standard di peso massimale λ irriducibile.*

Dimostrazione. **Unicità.** Si suppone esistano due moduli V e W con tali richieste, di generatori v^+ e w^+, allora si prendono $x^+ := (v^+, w^+) \in V \oplus W$ e $Y := \mathscr{U}(L)x^+ \subseteq V \oplus W$. Allora Y è ciclico standard di peso massimale λ. Siano p_V e p_W le proiezioni di Y su V e W; banalmente sono morfismi di L-moduli e le immagini contengono sicuramente v^+ e w^+. Per l'irriducibilità, le proiezioni sono suriettive, perciò esistono $M, N \subseteq Y$ tali che ${}^{Y}\!/_{M} \cong V$ e ${}^{Y}\!/_{N} \cong W$. Ma per il teorema 2.7.7, un modulo ciclico standard ha un unico quoziente irriducibile a meno di isomorfismo, da cui $V \cong W$.

Esistenza. Si definisce un $\mathscr{U}(B(\Delta))$-modulo, $D_\lambda := \langle p \rangle$, imponendo che le azioni su p siano date da $x_\alpha p = 0$ e $hp = \lambda(h)p$. Si considera allora $V := \mathscr{U}(L) \otimes_{\mathscr{U}(B(\Delta))} D_\lambda$ e si verifica che questo è un modulo ciclico standard di peso massimale λ. Il suo unico quoziente irriducibile è il modulo irriducibile cercato. □

24.05.2007

Definizione 2.7.9. A seguito del teorema, si denota con $V(\lambda)$ l'unico (a meno di isomorfismi) L-modulo irriducibile, standard, ciclico con peso massimale λ e vettore di peso massimale v^+.

Lemma 2.7.10. *Per $k \geq 0$, si hanno in $\mathscr{U}(L)$ le seguenti identità:*
$$\begin{aligned}
&[x_j, y_i^{k+1}] = 0 \text{ per } i \neq j,\\
&[h_j, y_i^{k+1}] = -(k+1)\alpha_i(h_j) y_i^{k+1},\\
&[x_i, y_i^{k+1}] = -(k+1) y_i^{k+1}(k \cdot 1 - h_i).
\end{aligned}$$

Dimostrazione. La prima identità viene dal fatto che $[x_j, y_i] \in L_{\alpha_i - \alpha_j}$ e se α_i e α_j sono radici diverse di una base, allora $\alpha_i - \alpha_j$ non è una radice (perché avrebbe almeno un coefficiente negativo e uno positivo), quindi $L_{\alpha_i - \alpha_j} = 0$; eventualmente si itera il procedimento.

La seconda si fa per induzione: il passo base è per definizione, quello induttivo:

$$\begin{aligned}[h_j, y_i^{k+1}] &= h_j y_i^{k+1} - y_i^{k+1} h_j = [h_j, y_i^k] y_i + y_i^k h y_i - y_i^k y_i h = \\ &= -k\alpha_i(h_j) y_i^{k+1} + y_i^k [h_j, y_i] = -k\alpha_i(h_j) y_i^{k+1} - \alpha_i(h_j) y_i^{k+1}.\end{aligned}$$

Per la terza, si scrive

$$[x_i, y_i^{k+1}] = x_i y_i^{k+1} - y_i^{k+1} x_i = [x_i, y_i] y_i^k + y_i [x_i, y_i^k] = h_i y_i^k + y_i [x_i, y_i^k]$$

e si procede per induzione usando anche la seconda identità. □

Teorema 2.7.11. *Gli L-moduli irriducibili di dimensione finita sono tutti e soli i $V(\lambda)$ con λ intero dominante, cioè $\lambda(h_{\alpha_i}) \in \mathbb{N}$ per ogni $\alpha_i \in \Delta$.*

Dimostrazione. $\Rightarrow$ Siano V un L-modulo irriducibile e v^+ un suo vettore massimale, che sicuramente esiste; allora $\mathscr{U}(L)v^+$ è un sottomodulo non nullo di V, da cui $\mathscr{U}(L)v^+ = V$ per l'irriducibilità. Ma $\mathscr{U}(L)v^+ = V(\lambda)$, dove λ è il peso di v^+.

Rimane da dimostrare che λ è intero dominante. Per ogni radice α_i, si considera V come un $\mathfrak{sl}(2,\mathbb{C})$-modulo, dove $\mathfrak{sl}(2,\mathbb{C})$ è la copia $\langle x_i, y_i, h_i\rangle$. Come $\mathfrak{sl}(2,\mathbb{C})$-modulo, V ha ancora come vettore di peso massimale v^+ di peso λ; ma per il teorema di struttura, $h_i v^+ = \lambda(h_i) v^+ \in \mathbb{N}$.

$\Leftarrow$ Sia $V(\lambda)$ il modulo ciclico standard di vettore di peso massimale v^+ di peso λ. Si pone $S_i := \langle x_i, y_i, h_i\rangle \cong \mathfrak{sl}(2,\mathbb{C})$. Si è già dimostrato che $V(\lambda)$ è irriducibile, si deve mostrare che ha dimensione finita.

1. Fissato i, $\left\langle v^+, y_i v^+, \dots, y_i^k v^+, \dots\right\rangle$ è un S_i-modulo di dimensione finita: siano $m := \lambda(h_i)$ e $w := y_i^{m+1} v^+$, allora dalla prima identità del lemma 2.7.10 e dal fatto che v^+ è massimale si ha $x_j w = [x_j, y_i^{k+1}] v^+ + y_i^{k+1} x_j v^+ = 0$; d'altra parte, dalla seconda e dalla terza identità,

   $$x_i w = y_i^{k+1} x_i v^+ - (m+1) y_i^m (m v^+ - \lambda(h_i) v^+) = 0.$$

   Essendo annullato da tutto gli x_k, w sarebbe un vettore massimale di peso $\lambda - (m+1)\alpha_i \neq \lambda$, assurdo per il teorema 2.7.7.

2. Sempre fissato i, si dimostra che $V(\lambda)$ è somma di S_i-moduli di dimensione finita. Sia V' la somma di tutti gli S_i-sottomoduli finiti di $V(\lambda)$ per qualche i; $V' \neq \varnothing$, dato che il primo punto dà un S_i-sottomodulo finito.

   Sia W uno di questi S_i-sottomoduli finiti; allora $W' := \sum_{\alpha\in\Phi^+}(x_\alpha W + y_\alpha W)$ è ancora un S_i-modulo: infatti $[x_i, x_\alpha W] = x_{\alpha_i+\alpha} W$ e così via: l'azione di S_i non fa uscire da W'. Inoltre W' è chiaramente finito.

   Di conseguenza, V' è stabile per L, cioè è un sottomodulo di V; essendo non vuoto, deve risultare $V' = V$ per l'irriducibilità.

3. Siano $\sigma_i(\alpha) := \alpha - \alpha(h_i)\alpha_i$ la riflessione rispetto a α_i e $s_i := e^{\rho(x_i)} e^{\rho(-y_i)} e^{\rho(x_i)}$ (dove $\rho\colon L \to \mathfrak{gl}(V(\lambda))$ è l'azione); la definizione di s_i ha senso perché $\rho(x_i)$ e $\rho(y_i)$ sono localmente nilpotenti (cioè,

per ogni v esiste $m(v) \in \mathbb{N}$ tale che $\rho(x_i)^{m(v)}v = 0 = \rho(y_i)^{m(v)}$), dato che v appartiene a una somma finita di S_i-moduli di dimensione finita, perciò i pesi dei vettori di questa somma non possono diventare arbitrariamente grandi.

Ora, si dimostra che se V_μ è uno spazio peso di $V(\lambda)$, si ha $s_i V_\mu = V_{\sigma_i \mu}$, cioè il gruppo di Weyl, generato dalle riflessioni, agisce sugli spazi peso. Innanzitutto, si osserva che se $g, h \in L$ e $\rho(g)$ è localmente nilpotente, allora $e^{\rho(g)}\rho(h)e^{-\rho(g)} = e^{\mathrm{ad}(\rho(g))}(\rho(h))$; infatti, $\mathrm{ad}(\rho(g)) = L_{\rho(g)} + R_{-\rho(g)}$ è somma di due operatori che commutano, da cui $e^{\mathrm{ad}(\rho(g))} = e^{L_{\rho(g)}}e^{R_{-\rho(g)}} = L_{e^{\rho(g)}}R_{e^{-\rho(g)}}$.

A questo punto, si ha

$$\begin{aligned}
s_i\rho(h_j)s_i^{-1} &= e^{\rho(x_i)}e^{\rho(-y_i)}e^{\rho(x_i)}\rho(h_j)e^{-\rho(x_i)}e^{\rho(y_i)}e^{-\rho(x_i)} = \\
&= e^{\mathrm{ad}(\rho(x_i))}e^{\mathrm{ad}(-\rho(y_i))}e^{\mathrm{ad}(\rho(x_i))}(\rho(h_j)) = \\
&= \rho(e^{\mathrm{ad}(x_i)}e^{\mathrm{ad}(-y_i)}e^{\mathrm{ad}(x_i)}(h_j));
\end{aligned}$$

l'ultima uguaglianza deriva dal fatto che ρ è un morfismo di algebre di Lie.

Per concludere, si separano due casi. Se $j = i$, allora $s_i\rho(h_i)s_i^{-1} = \rho(-h_i) = -\rho(h_i)$, calcolando direttamente; di conseguenza, $s_i\rho(h_i) = -\rho(h_i)s_i$, che applicato a $w \in V_\mu$ dà

$$\begin{aligned}
\rho(h_i)s_i w &= -s_i\rho(h_i)w = -\mu(h_i)s_i w = \\
&= (\mu(h_i) - \mu(h_i)\alpha_i(h_i))s_i w = \sigma_i(\mu)(h_i)s_i w,
\end{aligned}$$

cioè il peso di $s_i w$ rispetto a α_i è $\sigma_i(\mu)$.

Nel secondo caso, $i \neq j$, si procede allo stesso modo, usando però la matrice di Cartan.

4. Per ogni peso μ, l'orbita dell'azione del gruppo di Weyl su V_μ comprende almeno un peso non negativo, grazie alla transitività dell'azione del gruppo di Weyl sulle camere. Infatti, se μ non ha coefficienti nulli, si ottiene subito il risultato; se ne ha, significa che appartiene al bordo di una camera e per transitività è possibile portarlo sul bordo di una camera relativa a un peso positivo.

   Ora, gli spazi peso hanno dimensione finita, il gruppo di Weyl è finito ed è fatto da riflessioni, quindi le orbite sono finite. Rimane da dimostrare che i pesi positivi sono finiti, ma questo è ovvio perché i pesi possono essere solo del tipo $\lambda - \sum k_i\alpha_i$ con $k_i \in \mathbb{N}$. □

3 Risultati ulteriori

29.05.2007

3.1 Decomposizione di Levi

Siano $\mathfrak{q}$ e $\mathfrak{m}$ algebre di Lie su K e sia $\sigma\colon \mathfrak{m} \to \mathfrak{gl}(\mathfrak{q})$ una rappresentazione di $\mathfrak{m}$ in $\mathfrak{q}$ tale che $\sigma(Y)$ sia una derivazione di $\mathfrak{q}$ per ogni $Y \in \mathfrak{m}$. Si definisce un bracket su $\mathfrak{q} \times \mathfrak{m}$: $[(X, Y), (X', Y')] := [[X, X'] + \sigma(Y)X' - \sigma(Y')X, [Y, Y']]$. Questo bracket rende $\mathfrak{q} \times \mathfrak{m}$ un'algebra di Lie, che si chiamerà il *prodotto semidiretto* di $\mathfrak{q}$ e $\mathfrak{m}$ rispetto a σ e si denota $\mathfrak{q} \times_\sigma \mathfrak{m}$.

Osservazione 3.1.1. Se $\sigma = 0$, si ha il normale prodotto diretto.

Si considerano $\mathfrak{q}' := \mathfrak{q} \times \{0\}$ e $\mathfrak{m}' := \{0\} \times \mathfrak{m}$: preso $(l, 0)$, si ha $[(l, 0), (X', Y')] = [[l, X'] - \sigma(Y')l, 0]$, quindi $\mathfrak{q}'$ è un ideale. Il secondo invece non è un ideale, ma solo una sottoalgebra. Si ha inoltre $\mathfrak{q}' \cap \mathfrak{m}' = 0$ e $\mathfrak{q}' + \mathfrak{m}' = \mathfrak{q} \times_\sigma \mathfrak{m}'$.

Si vorrebbe sapere se, dati $\mathfrak{q}$ ideale e $\mathfrak{m}$ sottoalgebra contenuti in un'algebra di Lie $\mathfrak{g}$, soddisfacenti $\mathfrak{q} + \mathfrak{m} = \mathfrak{g}$ e $\mathfrak{q} \cap \mathfrak{m} = \{0\}$, si può esprimere $\mathfrak{g}$ come prodotto semidiretto di $\mathfrak{q}$ e $\mathfrak{m}$. Questo è in effetti possibile: definendo $\sigma(Y)X := -[Y, X]$, σ è una rappresentazione di $\mathfrak{m}$ su $\mathfrak{q}$ e $\sigma(Y)$ è una derivazione (a meno del segno, è la mappa aggiunta). Allora $\tau(X, Y) := X + Y$ è un isomorfismo tra $\mathfrak{q} \times_\sigma \mathfrak{m}$ e $\mathfrak{g}$.

Definizione 3.1.2. Siano $\mathfrak{g}$ un'algebra di Lie e $\mathfrak{q} := \mathrm{Rad}(\mathfrak{g})$; una sottoalgebra $\mathfrak{m}$ tale che $\mathfrak{q} \cap \mathfrak{m} = \{0\}$ e $\mathfrak{q} + \mathfrak{m} = \mathfrak{g}$ si dice *sottoalgebra di Levi*; $\mathfrak{g} = \mathfrak{q} + \mathfrak{m}$ si chiama *decomposizione di Levi.*

Teorema 3.1.3 (Levi-Mal'čev)**.** *Siano* $\mathfrak{g}$ *un'algebra di Lie su* K*,* $\mathfrak{q} = \mathrm{Rad}\,\mathfrak{g}$*; allora* $\mathfrak{g}$ *ammette una sottoalgebra di Levi* $\mathfrak{m}$*.*

Si deve notare che lo spezzamento è come spazi vettoriali; per ricostruire il prodotto si deve inserire il prodotto semidiretto. Sicuramente, $\mathfrak{m} \cong \mathfrak{g}/\mathrm{Rad}\,\mathfrak{g}$, quindi in particolare $\mathfrak{m}$ è semisemplice (nell'accezione di avere il radicale nullo).

Il teorema seguente permette di dire che con le rappresentazione che già si conoscono, è possibile trovare le rappresentazioni di (quasi) ogni algebra.

Teorema 3.1.4. *Siano* $\mathfrak{g}$ *un'algebra di Lie complessa,* $\mathfrak{g}_s := \mathfrak{g}/\mathrm{Rad}\,\mathfrak{g}$ *e* V *una rappresentazione irriducibile di* $\mathfrak{g}$*. Allora* V *è della forma* $V_0 \otimes \Gamma$*, dove* V_0 *è una rappresentazione di* $\mathfrak{g}_s$ *(ossia una rappresentazione di* $\mathfrak{g}$ *nulla sul radicale) e* Γ *è una rappresentazione di dimensione* 1*.*

Dimostrazione. Si usa un lemma: dati un ideale $\mathfrak{h} \leq \mathfrak{g}$, una rappresentazione V di $\mathfrak{g}$ e $\lambda \in \mathfrak{h}^\star$, posto $W := \{\, v \in V \mid (\forall X \in \mathfrak{h}) X(v) = \lambda(X) \,\}$, si ha $Y(W) \subseteq W$ per ogni $Y \in \mathfrak{g}$. Si userà con $\mathfrak{h} = \mathrm{Rad}\,\mathfrak{g}$, mostrando che $W \neq \varnothing$, da cui per l'irriducibilità dovrà essere $W = V$. □

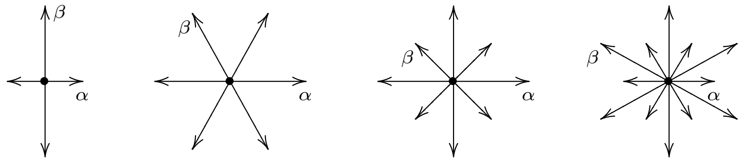
3.2 Teorema di Ado

Teorema 3.2.1 (Ado)**.** *Sia* $\mathfrak{g}$ *un'algebra di Lie di dimensione finita; allora esiste una rappresentazione fedele di dimensione finita di* $\mathfrak{g}$*.*

Sostanzialmente, il teorema di Ado dice che ogni algebra di Lie si può immergere in un gruppo lineare di qualche dimensione, anche se non specifica dei limiti per questa dimensione. La dimostrazione procede immergendo l'algebra in più passi: prima solo il centro, poi il radicale e poi tutta l'algebra.

Dal teorema di Ado, si ha che ogni algebra $\mathfrak{g}$ ammette un gruppo di Lie $G \subseteq \mathrm{GL}(n)$ tale che $G_e = \mathfrak{g}$. Questo però non dice che ogni gruppo di Lie è in realtà un gruppo lineare, dato che ci sono più gruppi che hanno la stessa algebra. Per i gruppi compatti invece si ha il seguente.

Teorema 3.2.2. *Ogni gruppo di Lie compatto ammette una rappresentazione fedele di dimensione finita.*



(a) $A_1 \times A_1$. (b) A_2. (c) B_2. (d) G_2.

Figura 1: Sistemi di radici in dimensione 2.

4 Complementi

27.03.2007

4.1 Sistemi di radici

Sia E uno spazio euclideo ($\mathbb{R}^n$ con un prodotto scalare).

Definizione 4.1.1. Una *riflessione* di E è un'applicazione $E \to E$ che fissa un iperpiano H e tale che per ogni $\alpha \perp H$, $\alpha \mapsto -\alpha$.

Fissato $v \in E$ e posto $\langle w, v\rangle := 2{}^{(w,v)}/_{(v,v)}$, $\sigma_v(w) := w - \langle w, v\rangle\, v$ è la riflessione rispetto all'iperpiano ortogonale a v.

Definizione 4.1.2. Un *insieme di radici* su E è un insieme $\Phi \subseteq E$ tale che:

1. Φ è un insieme finito che genera E e tale che $0 \notin \Phi$;
2. se $\alpha \in \Phi$, $\mathbb{R}\alpha \cap \Phi = \{\pm\alpha\}$;
3. se $\alpha \in \Phi$, $\sigma_\alpha(\Phi) = \Phi$;
4. se $\alpha, \beta \in \Phi$, $\langle \alpha, \beta\rangle \in \mathbb{Z}$.

Definizione 4.1.3. Il *gruppo di Weyl* di Φ è $W := \langle\, \sigma_\alpha \mid \alpha \in \Phi \,\rangle \subseteq \mathrm{O}(E)$.

Il gruppo di Weyl è sempre un gruppo finito: un suo elemento permuta le radici, quindi W si mappa nel gruppo delle permutazioni di Φ; la mappa è anche iniettiva perché le radici generano E, quindi due elementi di W che coincidono su Φ sono uguali.

Esempio 4.1.4. Sia $E = \mathbb{R}$; allora gli unici sistemi di radici sono del tipo $\{\pm\alpha\}$ e si denotano con A_1; su $\mathbb{R}^2$ le possibilità sono mostrate in figura 1.

Osservazione 4.1.5. Si può scrivere $(\alpha, \beta) = \|\alpha\|\,\|\beta\| \cos\vartheta$, da cui $\langle \alpha, \beta\rangle = 2\,{}^{\|\alpha\|}/_{\|\beta\|} \cos\vartheta$ e $\langle \alpha, \beta\rangle \langle \beta, \alpha\rangle = 4\cos^2\vartheta$. Essendo un intero, questo valore deve essere in $\{0, \pm1, \pm2, \pm3\}$, se si esclude il caso in cui α e β sono collineari.

$\lvert\langle \alpha, \beta\rangle\rvert$	$\lvert\langle \beta, \alpha\rangle\rvert$	ϑ	${}^{\|\beta\|^2}/_{\|\alpha\|^2}$
0	0	$\pi/2$	?
1	1	$\pi/3,\ 2/3\pi$	1
1	2	$\pi/4,\ 3/4\pi$	2
1	3	$\pi/6,\ 5/6\pi$	3

Da questa tabella, in cui sono mostrati i possibili casi a meno di scambiare α e β, si deduce che per ogni α e β non proporzionali e con $\cos(\alpha, \beta) \neq 0$, si ha che $\lvert\langle \alpha, \beta\rangle\rvert$ o $\lvert\langle \beta, \alpha\rangle\rvert$ è 1.

Inoltre, se $(\alpha, \beta) > 0$ (cioè se l'angolo tra α e β è strettamente acuto), allora $\alpha - \beta \in \Phi$; se $(\alpha, \beta) < 0$, allora $\alpha + \beta \in \Phi$. Infatti, se $(\alpha, \beta) > 0$, allora $\langle \alpha, \beta \rangle = 1$ o $\langle \beta, \alpha \rangle = 1$; se vale la prima, allora si ha $\alpha - \beta = \alpha - \langle \alpha, \beta \rangle \beta = \sigma_\beta(\alpha)$; altrimenti $-(\alpha - \beta) = \beta - \langle \beta, \alpha \rangle \alpha = \sigma_\alpha(\beta)$. Se $(\alpha, \beta) < 0$, si usa l'altro caso con $-\beta$ al posto di β.

Definizione 4.1.6. La *β-stringa* lungo α è l'insieme $\{\, \alpha + i\beta \mid i \in \mathbb{Z} \,\} \cap \Phi$.

Nella β-stringa lungo α, si avrà sicuramente un elemento massimo $\alpha + q\beta$ e uno minimo $\alpha + p\beta$. Tra questi ci sono tutti gli elementi possibili: se si suppone che ci siano $\alpha + r\beta$ e $\alpha + s\beta$ e che non ci siano $\alpha + (r+1)\beta, \dots, \alpha + (s-1)\beta$. Allora $(\alpha + s\beta, \beta) \leq 0$, $(\alpha + r\beta, \beta) \geq 0$ (altrimenti $\alpha + s\beta - \beta \in \Phi$ o $\alpha + r\beta + \beta \in \Phi$) e sottraendo si ottiene $(s\beta - r\beta, \beta) \leq 0$, da cui $s \leq r$ e quindi $s = r$.

Una β-stringa viene mandata in se stessa dalla riflessione σ_β: $\sigma_\beta(\alpha + \lambda\beta) = \alpha - \lambda\beta - \langle \alpha, \beta \rangle \beta$, che appartiene ancora alla stringa. Inoltre $\sigma_\beta(\alpha + p\beta) = \alpha - p\beta - \langle \alpha, \beta \rangle \beta = a + q\beta$, dato che la radice massima si ha per $\lambda = p$; questo significa che la stringa viene ribaltata dalla riflessione. Da questo si deduce anche che $|q - p| = |\langle \alpha, \beta \rangle| \leq 3$: una stringa è lunga al massimo 4 elementi e in generale la β-stringa lungo α è lunga $|\langle \alpha, \beta \rangle| + 1$ elementi.

Definizione 4.1.7. Un insieme $\Delta \subseteq \Phi$ si dice *base* di Φ se:

1. Δ è base per E;
2. per ogni $\beta \in \Phi$, $\beta = \sum_{\alpha \in \Delta} k_\alpha \alpha$ con i $k_\alpha \in \mathbb{Z}$ concordi o nulli.

In particolare, una radice β si dice *positiva* ($\beta > 0$) se i coefficienti sulla base sono tutti positivi o nulli, altrimenti di dirà che β è *negativa* ($\beta < 0$). Si avrà perciò una suddivisione $\Phi = \Phi^+ \sqcup \Phi^-$, che induce un ordinamento parziale su Φ: $\beta_1 < \beta_2$ se e solo se $\beta_2 - \beta_1 > 0$ (l'ordinamento non è totale perché non è detto che $\beta_2 - \beta_1$ rispetti la seconda condizione, dato che non è detto che sia una radice).

Teorema 4.1.8. *Esiste una base per Φ.*

Dimostrazione. Sia α una radice, si denota con P_α l'iperpiano $\{\, v \mid (v, \alpha) = 0 \,\}$. Si considera $E \setminus \bigcup_{\alpha \in \Phi} P_\alpha$, e si chiamano gli elementi di questo insieme *valori regolari*. Dato un valore regolare γ, si definisce $\Phi^+(\gamma) \coloneqq \{\, \alpha \in \Phi \mid (\alpha, \gamma) > 0 \,\}$ e allo stesso modo $\Phi^-(\gamma)$. Si ottiene una partizione di Φ (perché nessuna radice è ortogonale a γ) e da questa si vuole ottenere una base. Si dice che $\alpha \in \Phi^+(\gamma)$ è *decomponibile* se esistono $\beta_1, \beta_2 \in \Phi^+(\gamma)$ tali che $\alpha = \beta_1 + \beta_2$. Sia $\Delta(\gamma) \coloneqq \{\, \alpha \in \Phi^+(\gamma) \mid \alpha \text{ indecomponibile} \,\}$.

Sicuramente, qualsiasi radice di $\Phi^+(\gamma)$ è combinazione di radici di $\Delta(\gamma)$ con coefficienti tutti interi positivi o nulli, quindi anche qualsiasi elemento di Φ è combinazione di elementi di $\Delta(\gamma)$ con coefficienti interi e concordi, dato che $\Phi^- = -\Phi^+$. Ora, se α, β sono elementi distinti di $\Delta(\gamma)$, si ottiene che $(\alpha, \beta) \leq 0$; infatti, se fosse positivo, $\alpha - \beta$ sarebbe una radice e si considerano due casi: se $\alpha - \beta \in \Phi^+(\gamma)$, $\alpha = (\alpha - \beta) + \beta$ sarebbe decomponibile, altrimenti se $\beta - \alpha \in \Phi^+(\gamma)$, $\beta = \alpha + (\beta - \alpha)$ sarebbe decomponibile.

Si dimostra che $\Delta(\gamma)$ è fatto da vettori indipendenti: si suppone $\sum_{\alpha \in \Delta(\gamma)} k_\alpha \alpha = 0$; sia $\varepsilon \coloneqq \sum_{\alpha \in \Delta_1} k_\alpha \alpha = \sum_{\alpha \in \Delta_2} -k_\alpha \alpha$, dove Δ_1 è la parte di $\Delta(\gamma)$ fatta dagli elementi α con $k_\alpha > 0$, e Δ_2 dagli elementi α con $k_\alpha < 0$.

Allora $(\varepsilon, \varepsilon) \geq 0$ perché è una norma, ma $(\varepsilon, \varepsilon) \leq 0$ per l'osservazione precedente, quindi $\varepsilon = 0$. Perciò si può supporre che tutti i k_α siano positivi. Allora $0 = (\gamma, \varepsilon) = \sum_{\alpha \in \Delta(\gamma)} k_\alpha (\gamma, \alpha)$: dato che $k_\alpha \geq 0$ e $(\gamma, \alpha) > 0$, si deve avere che $k_\alpha = 0$ per ogni α. □

Osservazione 4.1.9. Con il procedimento visto nella dimostrazione, si possono ottenere tutte le possibili basi, scegliendo γ nelle varie componenti connesse. Scegliendo γ' nella stessa componente, chiaramente la base individuata è la stessa; d'altra parte se si sceglie γ' in un'altra componente, c'è almeno un iperpiano che separa i due punti, quindi le basi sono diverse. Per questo motivo, ci sono quindi tante basi quanti le componenti connesse di E meno gli iperpiani ortogonali agli elementi di Φ.

Definizione 4.1.10. Le componenti connesse di $E \setminus \bigcup_{\alpha \in \Phi} P_\alpha$ si dicono *camere di Weyl*.

Definizione 4.1.11. Fissata una base Δ, preso $\beta = \sum_{\alpha \in \Delta} k_\alpha \alpha$, si definisce l'*altezza* di β come $\operatorname{ht}(\beta) = \sum_{\alpha \in \Delta} k_\alpha$. Se $\beta \in \Delta$, $\operatorname{ht}(\beta) = 1$ e β è detta *semplice*.

Lemma 4.1.12. *Sia α una radice semplice; allora σ_α permuta $\Phi^+ \setminus \{\alpha\}$.*

Dimostrazione. Se $\beta \in \Phi^+ \setminus \{\alpha\}$, $\beta = \sum_{\gamma \in \Delta} k_\gamma \gamma$, con $k_\gamma \geq 0$ ed esiste almeno un $k_{\bar{\gamma}} > 0$ per un certo $\bar{\gamma} \neq \alpha$. Allora

$$\sigma_\alpha(\beta) = \beta - \langle \beta, \alpha \rangle \alpha = \beta - 2\frac{(\beta, \alpha)}{(\alpha, \alpha)}\alpha = \beta - 2\frac{\sum_{\gamma \in \Delta} k_\gamma (\gamma, \alpha)}{(\alpha, \alpha)}\alpha$$

appartiene ancora a Φ^+, dato che il coefficiente di $\bar{\gamma}$ è ancora strettamente positivo. Infine, la biunivocità è data da quella di σ_α. □

Lemma 4.1.13. *Siano $\alpha_1, \ldots, \alpha_k \in \Delta$ e si ponga $\sigma_i := \sigma_{\alpha_i}$. Se $\sigma_1 \cdots \sigma_{k-1}(\alpha_k) < 0$, allora $\sigma_1 \cdots \sigma_k = \sigma_1 \cdots \sigma_{s-1}\sigma_{s+1} \cdots \sigma_{k-1}$ per qualche s.*

Dimostrazione. Sia $\beta_i := \sigma_{i+1} \cdots \sigma_{k-1}(\alpha_k)$; allora $\beta_0 < 0$, ma $\beta_{k-1} = \alpha_k > 0$. Sia s il minimo per cui $\beta_s > 0$; si ha $\sigma_s \beta_s = \beta_{s-1} < 0$, ma per il lemma precedente, l'unica radice positiva che può essere mandata in una radice negativa da σ_s è α_s, cioè $\alpha_s = \beta_s = \sigma_{s+1} \cdots \sigma_{k-1}(\alpha_k) =: \tau(\alpha_k)$. Ora, si può dimostrare che $\sigma_{\tau(\alpha)} = \tau \sigma_\alpha \tau^{-1}$, perciò

$$\begin{aligned} \sigma_1 \cdots \sigma_k &= \sigma_1 \cdots \sigma_{s-1} \underbrace{(\sigma_{s+1} \cdots \sigma_{k-1})\sigma_k(\sigma_{k-1} \cdots \sigma_{s+1})}_{\sigma_s} \sigma_{s+1} \cdots \sigma_k = \\ &= \sigma_1 \cdots \sigma_{s-1}\sigma_{s+1} \cdots \sigma_{k-1}. \end{aligned}$$ □

Teorema 4.1.14. *Sia Δ una base di Φ, allora:*

1. *se γ è regolare, allora esiste $\sigma \in W$ tale che $(\sigma(\gamma), \alpha) > 0$ per ogni $\alpha \in \Delta$, cioè W agisce transitivamente sulle camere;*
2. *se Δ' è un'altra base di Φ, esiste $\sigma \in W$ tale che $\sigma(\Delta') = \Delta$, cioè W agisce transitivamente sulle basi;*
3. *se $\alpha \in \Phi$, esiste $\sigma \in W$ tale che $\sigma(\alpha) \in \Delta$;*
4. *$W = \langle \sigma_\alpha \mid \alpha \in \Delta \rangle =: W'$;*

5. *se σ fissa una base, allora $\sigma = \mathrm{Id}$.*

Dimostrazione. Si dimostrano inizialmente i primi tre punti per W'. Sia $\delta = {}^1\!/_2 \sum_{\alpha\in\Phi^+} \alpha$ e si prenda $\sigma \in W'$ tale che $(\sigma(\gamma), \delta)$ sia massimo. Se α è una radice semplice, $\alpha \in \Delta$ e $\sigma_\alpha \sigma \in W'$ e per la scelta di σ si ha

$$(\sigma(\gamma), \delta) \geq (\sigma_\alpha \sigma(\gamma), \delta) = (\sigma(\gamma), \sigma_\alpha^{-1}(\delta)) = \left(\sigma(\gamma), \delta - 2\frac{(\delta, \alpha)}{(\alpha, \alpha)}\alpha\right) =$$
$$= (\sigma(\gamma), \delta - \alpha) = (\sigma(\gamma), \delta) - (\sigma(\gamma), \alpha)$$

allora $(\sigma(\gamma), \alpha) \geq 0$ e non può essere nullo per la regolarità di γ.

Per il secondo punto, si usa la corrispondenza tra basi e camere. Per il terzo, siano α una radice e $\gamma \in P_\alpha \setminus \bigcup_{\beta\in\Phi^+\setminus\{\alpha\}} P_\beta$. Invece di γ, si usa γ' vicino a γ tale che $(\gamma', \alpha) = \varepsilon > 0$ e $|(\gamma', \beta)| > \varepsilon$ per ogni $\beta \neq \alpha$. In $\Phi^+(\gamma')$ necessariamente α è indecomponibile, quindi è un elemento di $\Delta(\gamma')$.

Sia ora $\beta \in \Phi$; per il terzo punto, esiste $\sigma \in W'$ tale che $\sigma(\beta) \in \Delta$. Ora, come già detto, $\sigma_{\sigma(\beta)} = \sigma\sigma_\beta\sigma^{-1}$, da cui $\sigma_\beta = \sigma^{-1}\sigma_{\sigma(\beta)}\sigma \in W'$.

Infine, sia σ che fissa una base Δ; se per assurdo $\sigma \neq \mathrm{Id}$, per il punto precedente si può scrivere $\sigma = \sigma_1 \cdots \sigma_k$ con k minimo e $\sigma_i \coloneqq \sigma_{\alpha_i}$, $\alpha_i \in \Delta$. Ora, da $\sigma_1 \cdots \sigma_k(\alpha_k) > 0$ si ottiene $\sigma_1 \cdots \sigma_{k-1}(\alpha_k) < 0$ (perché $\sigma_k(\alpha_k) = -\alpha_k$) e applicando il lemma precedente si può accorciare il prodotto contraddicendo l'ipotesi che k fosse minimo. □

Definizione 4.1.15. Data $\sigma \in W$, $\sigma = \sigma_1 \cdots \sigma_k$ con $\sigma_i \coloneqq \sigma_{\alpha_i}$, $\alpha_i \in \Delta$, si definisce la *lunghezza* di σ, $\mathrm{l}(\sigma)$ come la lunghezza della più piccola scrittura di quel tipo.

Si definisce $\mathrm{n}(\sigma) \coloneqq |\{\, \alpha \in \Phi^+ \mid \sigma(\alpha) \in \Phi^- \,\}|$.

Lemma 4.1.16. *Si ricava* $\mathrm{l}(\sigma) = \mathrm{n}(\sigma)$.

Dimostrazione. Per induzione su $\mathrm{l}(\sigma)$: se la lunghezza è nulla è chiaramente vero; se è maggiore di 0, si scrive $\sigma = \sigma_1 \cdots \sigma_p$; allora $\sigma(\alpha_p) < 0$, altrimenti si potrebbe accorciare la scrittura. Di conseguenza $\mathrm{n}(\sigma\sigma_p) = \mathrm{n}(\sigma) - 1$ (perché applicando σ_p tutte le radici positive tranne α_p si permutano tra loro, l'unica cosa che cambia è che $\sigma(\alpha_p) < 0$ mentre $\sigma\sigma_p(\alpha_p) > 0$); d'altra parte $\mathrm{l}(\sigma\sigma_p) = \mathrm{l}(\sigma) - 1$, quindi per induzione si ha la tesi. □

Esercizio 4.1.17. In W esiste un unico elemento w_Δ di lunghezza massima e soddisfa $\mathrm{l}(w_\Delta) = |\Phi^+|$.

03.04.2007

Definizione 4.1.18. Un insieme di radici Φ è *irriducibile* se $\Phi = \Phi_1 \sqcup \Phi_2$ con $\Phi_1 \perp \Phi_2$ implica $\Phi_1 = \varnothing$ o $\Phi_2 = \varnothing$.

Definizione 4.1.19. Una base Δ di Φ è *irriducibile* se $\Delta = \Delta_1 \sqcup \Delta_2$ con $\Delta_1 \perp \Delta_2$ implica $\Delta_1 = \varnothing$ o $\Delta_2 = \varnothing$.

Osservazione 4.1.20. Si osserva che vi è corrispondenza tra i due concetti di irriducibilità.

Se Φ non è irriducibile, $\Phi = \Phi_1 \sqcup \Phi_2$ con $\Phi_1 \perp \Phi_2$ non vuoti e posto $\Delta_i \coloneqq \Delta \cap \Phi_i$ si ha $\Delta_1 \perp \Delta_2$ e $\Delta_i \neq \varnothing$, dato che se $\Delta \subseteq \Phi_1$, Φ_2 sarebbe ortogonale rispetto a tutto E, assurdo.

Viceversa, se $\Delta = \Delta_1 \sqcup \Delta_2$, si pone Φ_i l'insieme delle radici con un coniugato in Δ_i (cioè, la cui W-orbita interseca Δ_i). Si osserva che se $v \in \Delta_1$ e $w \in \Delta_2$, allora $(v, w) = 0$ e di conseguenza le riflessioni σ_v e σ_w commutano. Ora, sia $\beta \in \Phi_1$, cioè $\beta = \sigma(\alpha_0)$ con $\alpha_0 \in \Phi_1$; si può supporre che $\sigma = \sigma_1 \cdots \sigma_k$, dove $\sigma_1, \dots, \sigma_r \in \Delta_2$ e $\sigma_{r+1}, \dots, \sigma_k \in \Delta_1$, per la commutatività. Allora, se $\sigma_i \in \Delta_1$ e $\alpha \in \Phi_1$, $\sigma_i(\alpha) = \alpha - \langle \alpha, \alpha_i \rangle \alpha_i \in \Phi_1$; invece, se $\sigma_i \in \Delta_2$ e $\alpha \in \Phi_1$, $\sigma_i(\alpha) = \alpha$. Si è ottenuto che $\beta \in \langle \Delta_1 \rangle$, cioè $\Phi_1 \subseteq \langle \Delta_1 \rangle$, e la stessa cosa per Φ_2. Con questo si mostra che $\Phi_1 \cap \Phi_2 = \varnothing$ e che $(\Phi_1, \Phi_2) = 0$.

Osservazione 4.1.21. La decomposizione in irriducibili di Φ è unica.

Lemma 4.1.22. *Sia Φ irriducibile, allora esiste una unica radice β di Φ tale che*

1. $\mathrm{ht}(\alpha) < \mathrm{ht}(\beta)$ *per ogni $\alpha \in \Delta$ diverso da β;*
2. $(\alpha, \beta) \geq 0$ *per ogni $\alpha \in \Delta$;*
3. $\beta = \sum_{\alpha \in \Delta} k_\alpha \alpha$ *con $k_\alpha > 0$ per ogni α.*

Dimostrazione. Sia $\beta = \sum_{\alpha \in \Delta} k_\alpha \alpha$ una radice di altezza massimale; si osserva innanzitutto che $(\beta, \alpha) \geq 0$, altrimenti $\alpha + \beta$ sarebbe radice, contraddicendo l'ipotesi di massimalità; in particolare, $k_\alpha \geq 0$, cioè $\beta > 0$. Si pongono $\Delta_1 := \{\, \alpha \in \Delta \mid k_\alpha > 0 \,\}$ e $\Delta_2 := \{\, \alpha \in \Delta \mid k_\alpha = 0 \,\}$. Se $\Delta_2 \neq \varnothing$, per ogni $\alpha \in \Delta_2$, $(\alpha, \beta) \leq 0$, perché il prodotto scalare di due elementi distinti di una base è non positivo. D'altra parte, $(\alpha, \beta) \geq 0$, quindi deve essere $(\alpha, \beta) = 0$ per ogni $\alpha \in \Delta_2$; ma questo è impossibile perché si avrebbe una partizione di Δ in due insiemi ortogonali tra loro. Perciò deve essere $\Delta_2 = \varnothing$, cioè $k_\alpha > 0$ per ogni α.

Poiché Δ genera E, deve esistere $\alpha \in \Delta$ tale che $(\alpha, \beta) > 0$. Si suppone $\beta' = \sum_{\alpha \in \Delta} k'_\alpha \alpha$ massimale: allora $(\beta, \beta') = \sum_{\alpha \in \Delta} (\beta, \alpha) k'_\alpha > 0$ (perché $k'_\alpha > 0$, $(\beta, \alpha) \geq 0$ e uno di questi sicuramente è non nullo). Allora $\beta - \beta' \in \Phi \cup \{0\}$, cioè $\beta < \beta'$ o $\beta > \beta'$ o $\beta = \beta'$, ma per la massimalità le altezze sono uguali, perciò si deve verificare il terzo caso. □

Lemma 4.1.23. *Sia Φ irriducibile; si hanno al massimo due norme distinte per le radici. Tutte le radici con stessa norma sono coniugate tramite W.*

Dimostrazione. Preso $\alpha \in \Phi$, si ha che $\langle W\alpha \rangle = E$: se non fosse vero, si avrebbe una decomposizione non banale $\langle W\alpha \rangle \oplus \langle W\alpha \rangle^\perp = E$, da cui Φ sarebbe riducibile (definendo $\Phi_1 := \Phi \cap \langle W\alpha \rangle$), assurdo.

Presi $\alpha, \beta \in \Phi$, a meno di agire con W si può supporre $(\alpha, \beta) \neq 0$, dato che se $\beta \perp v$ per ogni $v \in \langle W\alpha \rangle = E$, allora $\beta = 0$. Quindi ${}^{\|\alpha\|}/_{\|\beta\|} \in \{1/3, 1/2, 1, 2, 3\}$; supponendo $\|\alpha\| \geq \|\beta\|$, la frazione può essere solo 1, 2, 3. Se ci fossero state tre norme distinte, con $\|\alpha\|$ massima, allora le altre due avrebbero rapporto $1/2$ e $1/3$, quindi tra di loro $3/2$, ma questo non è ottenibile.

Se $\|\alpha\| = \|\beta\|$, si può supporre $(\alpha, \beta) \neq 0$, $\langle \alpha, \beta \rangle = \langle \beta, \alpha \rangle = 1$ (a meno di prendere l'opposto di α). Quindi $\sigma_\alpha \sigma_\beta \sigma_\alpha(\beta) = \sigma_\alpha \sigma_\beta(\beta - \alpha) = \sigma_\alpha(-\beta - \alpha + \beta) = \sigma_\alpha(-\alpha) = \alpha$. □

Definizione 4.1.24. Data una base $\Delta := \{\alpha_1, \dots, \alpha_k\}$, la *matrice di Cartan* associata a Δ è $M := (\langle \alpha_i, \alpha_j \rangle)_{1 \leq i,j \leq k}$.

Proposizione 4.1.25. *La matrice di Cartan determina Φ a meno di isomorfismi.*

(a) $A_1 \times A_1$. (b) A_2. (c) B_2. (d) G_2.

Figura 2: Grafi di Coxeter per sistemi di radici in dimensione 2.

Definizione 4.1.26. Il *grafo di Coxeter* di (Φ, Δ) ha come vertici gli elementi di Δ e per ogni $i \neq j$, (α_i, α_j) è un lato di molteplicità $\langle \alpha_i, \alpha_j \rangle \langle \alpha_j, \alpha_i \rangle$.

Definizione 4.1.27. Il *diagramma di Dynkin* è un grafo di Coxeter con i lati orientati dalle radici di lunghezza più piccola.

Esempio 4.1.28. Le matrici di Cartan e i grafi di Coxeter (in figura 2) per i sistemi di radici in dimensione 2:

1. $A_1 \times A_1$ ha $M = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$ e grafo di Coxeter formato da due punti sconnessi;
2. A_2 ha $M = \left(\begin{smallmatrix} 2 & -1 \\ -1 & 2 \end{smallmatrix}\right)$ e grafo di Coxeter formato da due punti uniti da un lato;
3. B_2 ha $M = \left(\begin{smallmatrix} 2 & -2 \\ -1 & 2 \end{smallmatrix}\right)$ e grafo di Coxeter formato da due punti uniti da un lato doppio;
4. G_2 ha $M = \left(\begin{smallmatrix} 2 & -3 \\ -1 & 2 \end{smallmatrix}\right)$ e grafo di Coxeter formato da due punti uniti da un lato triplo.

Osservazione 4.1.29. Se Φ è riducibile, allora il grafo di Coxeter è sconnesso.

Proposizione 4.1.30. *Se Φ è irriducibile, il suo diagramma di Dynkin è uno tra $\{ A_n \mid n \geq 1 \}$, $\{ B_n \mid n \geq 2 \}$, $\{ C_n \mid n \geq 3 \}$, $\{ D_n \mid n \geq 4 \}$ o tra i grafi speciali E_6, E_7, E_8, F_4, G_2, rappresentati in figura 3.*

Dimostrazione. Si classificano innanzitutto i grafi irriducibili di Coxeter, per cui non è importante la norma delle radici; si dice che un sistema

di radici $\{\varepsilon_i\}$ è ammissibile se è una base di E con $\|\varepsilon_i\| = 1$, $(\varepsilon_i, \varepsilon_j) \leq 0$, $4(\varepsilon_i, \varepsilon_j)^2 \in \{0, 1, 2, 3\}$ per $i \neq j$; un grafo ammissibile è un grafo di un sistema di radici ammissibile. Si osservano le seguenti.

1. Se un grafo è ammissibile lo è anche un suo sottografo.
2. Il numero di coppie di vertici connessi da almeno un lato è minore di n: se $\varepsilon := \sum \varepsilon_i$, dato che le radici sono indipendenti si ha $0 < (\varepsilon, \varepsilon) = n + 2\sum_{i<j} (\varepsilon_i, \varepsilon_j)$; inoltre se $(\varepsilon_i, \varepsilon_j) \notin \{0, 1\}$ (cioè se i vertici ε_i e ε_j sono distinti e connessi da un lato), si ha $4(\varepsilon_i, \varepsilon_j)^2 \in \{1, 2, 3\}$ e da questo $2(\varepsilon_i, \varepsilon_j) \leq -1$; per la disuguaglianza, il numero di tali coppie, che sono quelle collegate da un arco, deve essere minore di n.
3. Non ci sono cicli, poiché originerebbero un sottografo di k vertici e k lati, assurdo per le precedenti osservazioni.
4. Da un vertice non possono uscire più di tre lati: sia ε un vertice e $\eta_1, \ldots, \eta_k$ i vertici a lui connessi, allora $(\varepsilon, \eta_i) < 0$ e il fatto che non ci siano cicli dà $(\eta_i, \eta_j) = 0$. Per l'indipendenza, esiste $\eta_0 \in \langle \varepsilon, \eta_1, \ldots, \eta_k \rangle$ ortogonale

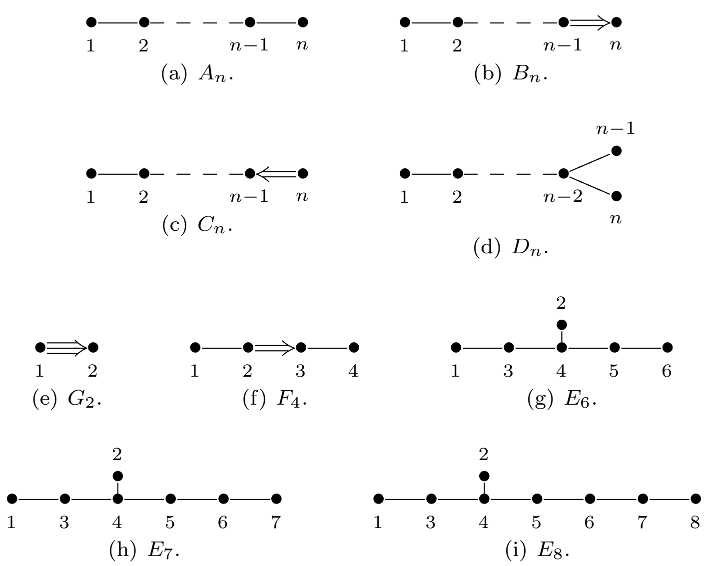


Figura 3: I possibili sistemi di radici.

a tutti gli η_i e di norma unitaria, da cui $(\eta_0, \varepsilon) \neq 0$; di conseguenza $\varepsilon = \sum_{i=0}^{k} (\varepsilon, \eta_i)\eta_i$ e

$$1 = (\varepsilon, \varepsilon) = \sum_{i=0}^{k} (\varepsilon, \eta_i)^2 = (\varepsilon, \eta_0)^2 + \sum_{i=1}^{k} (\varepsilon, \eta_i)^2,$$

ma $(\varepsilon, \eta_0) \neq 0$, quindi $\sum_{i=1}^{k} 4(\varepsilon, \eta_i)^2 < 4$ e $4(\varepsilon, \eta_i)^2$ è il numero di archi che collegano ε con η_i.

5. Come conseguenza immediata, l'unico grafo con un lato triplo è G_2.

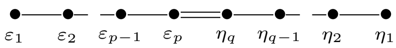
6. Se si suppone che nel grafo ammissibile sia contenuto un sottografo lineare di vertici $\varepsilon_1, \ldots, \varepsilon_k$, "contraendo" questi vertici a $\varepsilon := \sum \varepsilon_i$, si ottiene ancora un grafo ammissibile. Infatti

$$(\varepsilon, \varepsilon) = \sum_{i=1}^{k-1} 2(\varepsilon_i, \varepsilon_{i+1}) = k - (k-1) = 1$$

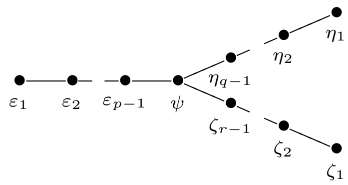
e se η è un altro vertice, $(\varepsilon, \eta) = 0$ se $(\varepsilon_i, \eta) = 0$ per ogni i, altrimenti vale (ε_j, η) se ε_j è l'unico per cui il prodotto scalare è non nullo (non possono essercene di più per la condizione sui cicli).

7. Non si possono avere configurazioni lineari che presentano a entrambi gli estremi lati doppi o biforcazioni, altrimenti si potrebbero contrarre gli archi interni e ottenere un nodo con 4 archi uscenti.

8. In un grafo c'è al più uno tra archi doppi e biforcazioni, altrimenti un sottografo sarebbe del tipo impedito dal punto precedente; di conseguenza gli ultimi casi da eliminare sono quelli di figura 4.



(a) Primo caso.



(b) Secondo caso.

Figura 4: Ultimi casi da eliminare.

9. Nel primo caso, siano $\varepsilon \coloneqq \sum i\varepsilon_i$ e $\eta \coloneqq \sum i\eta_i$, allora

$$(\varepsilon, \varepsilon) = \sum_{i=1}^{p} i^2 - \sum_{i=1}^{p-1} i(i+1) = \frac{p(p+1)}{2}$$

e così $(\eta, \eta) = {}^{q}\!/\!{}_{2}(q+1)$. D'altra parte $(\varepsilon, \eta)^2 = {}^{1}\!/\!{}_{2}p^2q^2$ e deve verificarsi $(\varepsilon, \eta)^2 < (\varepsilon, \varepsilon)(\eta, \eta)$ (il segno stretto viene dal fatto che ε e η sono indipendenti), cioè $(p-1)(q-1) < 2$, quindi gli unici casi possibili sono B_{n+1}, per $\{p, q\} = \{1, n\}$ e F_2 per $\{p, q\} = \{2\}$.

10. Per il secondo caso, siano ϑ_1, ϑ_2, ϑ_3 gli angoli tra ψ e ε_{p-1}, η_{q-1} e ζ_{r-1}, allora $\sum \cos(\vartheta_i) < 1$ come mostrato nel punto 4, da cui ${}^{1}\!/\!{}_{p} + {}^{1}\!/\!{}_{q} + {}^{1}\!/\!{}_{r} > 1$: gli unici casi possibili sono $(p, q, r) = (2, 2, n)$, che corrisponde a D_{n+1} e $(2, 3, 3)$, $(2, 3, 4)$ e $(2, 3, 5)$ che corrispondono a E_6, E_7, E_8. □

Teorema 4.1.31. *Per ciascun diagramma di Dynkin tra quelli elencati esiste un sistema di radici corrispondente.*

Dimostrazione. Si mostrerà solo per i diagrammi delle famiglie infinite.

1. Per A_n, sia $E \coloneqq \mathbb{R}^{n+1}$, (ε_i) la base standard e $\Phi \coloneqq \{\, \varepsilon_i - \varepsilon_j \mid i \neq j \,\}$, $W = S_{n+1}$; l'algebra di Lie corrispondente è $\mathfrak{sl}(n+1, \mathbb{C})$.

2. Per B_n, si prende $E \coloneqq \mathbb{R}^n$, $\Phi \coloneqq \{\pm\varepsilon_i, \pm\varepsilon_i \pm \varepsilon_j\}$, W è formato dalle permutazioni e dai cambi di segno su n coordinate; l'algebra di Lie associata è $\mathfrak{so}(2n+1, \mathbb{C})$.

3. Per C_n, si prende $E \coloneqq \mathbb{R}^n$, $\Phi \coloneqq \{\pm 2\varepsilon_i, \pm\varepsilon_i \pm \varepsilon_j\}$, W è sempre formato dalle permutazioni e dai cambi di segno su n coordinate; l'algebra di Lie è $\mathfrak{sp}(2n, \mathbb{C})$.

4. Per D_n, si ha $E \coloneqq \mathbb{R}^n$, $\Phi \coloneqq \{\pm\varepsilon_i \pm \varepsilon_j\}$, W è formato dalle permutazioni e dai cambi di segno pari su n coordinate e l'algebra di Lie associata è $\mathfrak{so}(2n, \mathbb{C})$. □

4.2 Gruppi topologici

24.04.2007

Sia G un gruppo topologico, $\tilde{G}$ un rivestimento, cioè $p \colon \tilde{G} \to G$ con $p^{-1}(x)$ discreto e tale che p è localmente banale (per ogni $x \in G$ esiste un intorno U tale che $p^{-1}(U) \approx p^{-1}(x) \times U$). Ci si chiede se si può considerare una struttura di gruppo sul rivestimento.

Teorema 4.2.1. *Sia $\omega\colon G^\star \to G$ un rivestimento con $G^\star$ uno spazio topologico e G un gruppo topologico, entrambi connessi per archi e localmente connessi per archi. Allora esiste una struttura di gruppo su $G^\star$ che rende ω un morfismo di gruppi topologici.*

Dimostrazione. Sia $e \in G$ l'identità. Si sceglie l'identità $e^\star \in \omega^{-1}(e) \subseteq G^\star$ e poi si definisce il prodotto $a^\star b^\star$. Si considerano $f^\star, g^\star\colon I \to G^\star$ cammini con partenza in $e^\star$ e arrivo rispettivamente in $a^\star$ e $b^\star$. Si possono prendere $f \coloneqq \omega f^\star$ e $g \coloneqq \omega g^\star$ e $h \coloneqq fg\colon I \to G\colon t \mapsto f(t)g(t)$, cammino con partenza in e e arrivo in ab. Si può allora sollevare il cammino h a un cammino $h^\star$ in $G^\star$ che parte da $e^\star$. Allora si definisce $a^\star b^\star$ come $h^\star(1)$.

Bisogna dimostrare che questo valore non dipende dalle scelte fatte: se si considerano $f_1^\star$ e $g_1^\star$ si arriverà a un cammino $h_1^\star$; allora $h_1^{-1} \circ h \in \pi_1(G, e)$. Si deve dimostrare che $h_1^{-1} \circ h \in \omega_\star \pi_1(G^\star, e)$; h può essere visto come la diagonale di un quadrato che ha come lati f, g, ag e bf, cioè $h = ag \circ f$ (composizione di cammini); allora $h_1^{-1} \circ h = f_1^{-1} \circ (ag_1)^{-1} \circ ag \circ f = f_1^{-1} \circ a(g_1^{-1} \circ g) \circ f \simeq f_1^{-1} \circ f \circ g_1^{-1} \circ g$ (considerando il quadrato di lati f, $g_1^{-1} \circ g$, $a(g_1^{-1} \circ g)$, f). Ora, $f_1^{-1} \circ f = \omega_\star({f_1^\star}^{-1} \circ f^\star)$ e lo stesso per g.

Bisogna ancora dimostrare l'esistenza dell'inversa (si procede allo stesso modo) e che ω è un morfismo di gruppi. □

Osservazione 4.2.2. La mappa ω è aperta e $\ker(\omega)$ è un sottogruppo normale e discreto di $G^\star$.

Definizione 4.2.3. Dati due gruppi topologici G_1 e G_2, $f\colon U_1 \to U_2$ con U_i intorno di e_i in G_i, allora f è un *morfismo locale di gruppi topologici* se:

1. $f(e_1) = e_2$;
2. f è continua;
3. per ogni $a, b \in U_1$ tali che $ab \in U_1$, $f(a)f(b) = f(ab)$.

Si vogliono determinare delle condizioni su un morfismo locale per poterlo estendere a un morfismo globale. Si può però considerare il rivestimento universale $\tilde{G_1}$ di G_1, da cui si potrà creare la mappa che estende il morfismo locale.

Teorema 4.2.4. *Siano G, G' gruppi topologici connessi per archi, G localmente connesso per archi e semplicemente connesso. Sia $f\colon U \to U'$ un morfismo locale. Allora esiste una unica mappa $\varphi\colon G \to G'$, morfismo di gruppi topologici che estende f inoltre:*

1. *f è suriettiva (nel senso che $f(U)$ contiene un intorno dell'identità) se e solo se φ è suriettiva;*
2. *f è aperta se e solo se φ lo è;*
3. *se G' è localmente connesso per archi e semplicemente connesso e se f è un isomorfismo locale, allora φ è un isomorfismo di gruppi.*

Dimostrazione. Se φ esiste e f è suriettiva, allora $\varphi(G) \supseteq f(U) \supseteq U'$, cioè l'immagine di φ contiene un intorno dell'identità di G'; ma G' è connesso per archi, quindi è generato da un suo intorno dell'identità. Il viceversa è banale.

Se f è aperta, φ è aperta: dato $\Omega \subseteq G$ aperto, allora Ω è unione di traslati di intorni dell'identità, la cui immagine è aperta per l'ipotesi su f. Il viceversa è ancora banale.

Se φ esiste è unica: se anche φ' estende f, sia $W := \{\varphi = \varphi'\} \supseteq U$; ma allora $\varphi = \varphi'$ su $\langle U \rangle = G$, per la connessione di G.

Se f è un isomorfismo locale e G' è semplicemente connesso, allora φ è un isomorfismo locale, quindi un rivestimento. Ma anche G è semplicemente connesso, quindi φ è un isomorfismo.

Si dimostra ora l'esistenza. Sia $g\colon I \to G$ un cammino con $g(0) = e$, a cui si vuole associare un cammino $g'\colon I \to G'$, in modo che $g'(0) = e'$ e se $t_1, t_2 \in I$, con $g(t_1)^{-1}g(t_2) \in U$, allora $f(g(t_1)^{-1}g(t_2)) = g'(t_1)^{-1}g'(t_2)$. Si definisce $g'(t') := g'(t)f(g(t)^{-1}g(t'))$ con t sufficientemente piccolo. Sia $[0, \tau]$ l'intervallo su cui si riesce a definire g'; allora esiste $\varepsilon > 0$ tale che per ogni t_1, t_2 con $|t_1 - t_2| < \varepsilon$, vale $g(t_1)^{-1}g(t_2) \subseteq U \cap U^{-1}$. Infatti, questo ε non è altro che il numero di Lebesgue dell'intervallo unitario col ricoprimento dato dalle controimmagini di U tramite le mappe $t \mapsto g(\bar{t})^{-1}g(t)$. Allora esiste un unico modo per estendere g': se $t - \tau < \varepsilon$, si pone $g'(t) := g'(\tau)f(g(\tau)g(t))$. Ma ε non dipende da τ, quindi si può estendere g' su tutto l'intervallo unitario.

Si potrebbe definire $\varphi(g(1)) := g'(1)$, ma si deve verificare che è una buona definizione. Siano g_1 e g_2 due cammini uguali ovunque tranne che in una parte contenuta in un traslato di U: cioè $g_1 = g_2$ fuori da $[t, t+\varepsilon]$ e $g_i(t)^{-1}g_i(t') \in U$ per $t' \in [t, t+\varepsilon]$. Ma allora $g_1'(1) = g_2'(1)$. Se invece g_1 e g_2 sono qualsiasi, si ha comunque un'omotopia a estremi fissi tra g_1 e g_2 (G è semplicemente connesso). Si ricopre il quadrato dell'omotopia con una griglia di quadrati con lato minore di ε, il numero di Lebesgue visto prima. Allora si può procedere deformando i cammini un quadrato alla volta e si ottiene ancora $g_1'(1) = g_2'(1)$. Quindi φ è ben definita e rimane da verificare solo che φ è un morfismo di gruppi. $\square$

Allora dato un morfismo locale $f\colon G \to G'$, questo non si può estendere sempre a un morfismo globale, ma si estende la mappa $f \circ \omega$, dove ω è il rivestimento universale di G. Da quanto visto segue facilmente la seguente.

Proposizione 4.2.5. *Se G_1 e G_2 sono gruppi topologici localmente isomorfi allora sono rivestiti da uno stesso gruppo $\tilde{G}$ semplicemente connesso.*

Si ha che $\ker(\omega)$ è un sottogruppo discreto e normale di $\tilde{G}$.

Proposizione 4.2.6. *Sia $N \leq G$ un sottogruppo discreto e normale di un gruppo topologico G connesso, allora $N \subseteq \mathrm{Z}(G)$.*

Dimostrazione. Siano $a \in N$ e V un intorno di a tale che $V \cap N = \{a\}$. Sia U un intorno di e in G tale che $U^{-1}aU \subseteq V$; allora, per ogni $u \in U$, $u^{-1}au \in V$, ma appartiene anche a N perché N è normale: $U^{-1}aU = \{a\}$, cioè a commuta con gli elementi di U, che per la connessione sono generatori di G, quindi a commuta con tutto G. $\square$

Da quanto detto finora, si ottiene il seguente risultato.

Proposizione 4.2.7. *Se G è un gruppo topologico, tutti i gruppi che sono localmente isomorfi a lui sono gruppi del tipo $\tilde{G}/N$ dove $\tilde{G}$ è il rivestimento universale e N è un sottogruppo discreto di $\mathrm{Z}(G)$.*

Definizione 4.2.8. Un gruppo topologico G si dice *ammissibile* se è connesso per archi, localmente connesso per archi, localmente semplicemente connesso e a base numerabile.

Teorema 4.2.9. *Siano G_1, G_2 gruppi topologici ammissibili, $\pi\colon G_1 \to G_2$ un morfismo continuo, suriettivo e con nucleo discreto, allora se G_1 (o G_2) è un gruppo di Lie, esiste un'unica struttura di gruppo di Lie su G_2 (o G_1) che rende π un morfismo di gruppi di Lie.*

Dimostrazione. L'unicità è già stata dimostrata in altra sede. Si vuole mostrare l'esistenza. La mappa π è un rivestimento (perché ha nucleo discreto). Per dare la struttura differenziale all'altro gruppo si può semplicemente sfruttare il fatto che π è localmente un fibrato triviale. Più rigorosamente, si porta la struttura differenziale su un intorno dell'identità con la mappa π, e poi si porta in tutto il gruppo grazie alla struttura di gruppo. □

Proposizione 4.2.10. *Due gruppi di Lie G_1 e G_2 sono localmente isomorfi se e solo se le loro algebre di Lie sono isomorfe.*

Dimostrazione. $\Rightarrow$ Se G_1 e G_2 sono localmente isomorfi allora sono rivestiti dallo stesso $\tilde{G}$ semplicemente connesso. Siano $\varphi_i\colon \tilde{G} \to G_i$ le proiezioni, allora φ_i' è un morfismo di algebre di Lie, ma è anche un isomorfismo perché φ è localmente un isomorfismo. □

Teorema 4.2.11. *Se G_1 e G_2 sono gruppi di Lie, $\lambda\colon \mathfrak{g}_1 \to \mathfrak{g}_2$ è un morfismo di algebre di Lie, allora esiste al più una mappa $\pi\colon G_1 \to G_2$ il cui differenziale è λ. In particolare, se G_1 è semplicemente connesso, π esiste.*

26.04.2007

Dimostrazione. Sia $G \coloneqq G_1 \times G_2$, allora $\mathfrak{g} = \mathfrak{g}_1 \times \mathfrak{g}_2$ e si definisce $\mathfrak{h} \coloneqq \Gamma_\lambda = \{\, (x, \lambda(x)) \mid x \in \mathfrak{g}_1 \,\}$. Si vorrebbe associare un gruppo $H \leq G$ con algebra di Lie $\mathfrak{h}$ ed effettivamente questo H esiste per la formula di Baker-Campbell-Hausdorff: $\exp(\mathfrak{h})\exp(\mathfrak{h}) \subseteq \exp(\mathfrak{h})$, cioè $\exp(\mathfrak{h})$ è un sottogruppo ed è facile osservare che la sua algebra è proprio $\mathfrak{h}$. Se esiste π, si considera l'applicazione $\sigma\colon G_1 \to G$ data da $\sigma(g_1) \coloneqq (g_1, \pi(g_1))$; allora $\sigma' = (\mathrm{Id}, \pi') = (\mathrm{Id}, \lambda)$: questa mappa dà un isomorfismo tra $\mathfrak{g}_1$ e $\mathfrak{h}$. Ora, G_1 è generato da $\exp(\mathfrak{g}_1)$ e H da $\exp(\mathfrak{h})$, quindi $H = \langle \sigma(G_1) \rangle$, dato che $H = \langle \exp(\sigma'(\mathfrak{g}_1)) \rangle = \langle \sigma \exp(\mathfrak{g}_1) \rangle = \langle \sigma(G_1) \rangle$. La mappa π determina in modo unico σ, che a sua volta determina in modo unico H e $\mathfrak{h}$; ancora, a $\mathfrak{h}$ corrisponde univocamente λ. Di conseguenza, se esiste, π è unica, perché univocamente determinata da λ.

Si suppone ora che G_1 sia semplicemente connesso, allora G si può proiettare su G_1 con la proiezione γ sulla prima coordinata. Questa dà una proiezione γ' da $\mathfrak{g}$ a $\mathfrak{g}_1$, perciò restringendo si ha $\gamma'_{|\mathfrak{h}}\colon \mathfrak{h} \to \mathfrak{g}_1$. Ma $\gamma'_{|\mathfrak{h}}$ è l'identità sulla prima coordinata, quindi $\gamma_{|H}$ è un rivestimento di G_1 (perché il differenziale è invertibile). Ma G_1 è semplicemente connesso, perciò anche H lo è ed è isomorfo a G_1. Considerando la proiezione su G_2, si può costruire $G_1 \to H \to G_2$, dove la prima mappa è l'inversa di $\gamma_{|H}$; allora la composizione $G_1 \to G_2$ ha differenziale λ. □

Si vogliono classificare i gruppi di Lie con diagrammi di Dynkin del tipo A_n, B_n, C_n, D_n.

Definizione 4.2.12. La mappa $p\colon E \to B$ ha *fibra* F se $p^{-1}(b) \approx F$ per ogni $b \in B$; p è un *fibrato localmente banale* se per ogni b esiste un intorno U tale che $p^{-1}(U) \approx U \times F$.

Se $F \xrightarrow{i} E \xrightarrow{p} B$ un fibrato di fibra F, a livello di gruppi di omotopia (fissando dei punti base) si possono considerare le mappe $\pi_n(F) \xrightarrow{i_\star} \pi_n(E) \xrightarrow{p_\star} \pi_n(B)$; in realtà questa è una successione esatta di gruppi che può essere completata a una successione esatta lunga di gruppi (fino a $\pi_1(B)$) o di insiemi (fino a $\pi_0(B)$).

Esempio 4.2.13. Si considera

$$\mathrm{SO}(2,\mathbb{C}) = \left\{ A \in \mathscr{M}_2(\mathbb{C}) \mid A^t M A = M, \det(A) = 1 \right\},$$

dove M è la matrice di un prodotto scalare, ad esempio $M = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Se $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, le condizioni danno che $b = c = 0$ e $d = a^{-1}$, da cui di ricava $\mathrm{SO}(2,\mathbb{C}) = \mathbb{C}^\star$, quindi ha gruppo fondamentale $\mathbb{Z}$.

Esempio 4.2.14. Per $\mathrm{SO}(3,\mathbb{C})$ si può prendere l'applicazione $\varphi\colon \mathbb{C}^3 \to \mathfrak{gl}(2,\mathbb{C})$ che associa a $(x_1,x_2,x_3) \in \mathbb{C}^3 \cong \mathrm{SL}(2,\mathbb{C})$ la somma $x_1 \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right) + x_2 \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) + x_3 \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$. L'immagine è costituita da matrici di traccia nulla, quindi da elementi di $\mathfrak{sl}(2,\mathbb{C})$. Ora si prende $\rho\colon \mathrm{SL}(2,\mathbb{C}) \to \mathrm{GL}(3,\mathbb{C})$, dove $\rho(A) \coloneqq (v \mapsto \varphi^{-1}(A^{-1}\varphi(v)A))$. Si dimostra facilmente che l'immagine di ρ è contenuta in $\mathrm{O}(3,\mathbb{C})$. Ma $\mathrm{SL}(2,\mathbb{C})$ si può proiettare su $\mathbb{C}^2 \setminus \{0\}$ mandando A in Ae_1 (si prende il primo vettore della base), e la fibra di questa proiezione è $\mathbb{C}$ (poiché ρ è anche un'azione di gruppi transitiva, le fibre sopra ogni punto sono omeomorfe e ρ è un fibrato). Questo permette di dire che $\mathrm{SL}(2,\mathbb{C})$ ha lo stesso gruppo di omotopia di $\mathbb{C}^2 \setminus \{0\}$, per considerazioni sulla successione esatta lunga

$$\ldots \to \{e\} = \pi_1(\mathbb{C}) \to \pi_1(\mathrm{SL}(2,\mathbb{C})) \to \pi_1(\mathbb{C}^2 \setminus \{0\}) = \pi_1(S^3) = \{e\}\,.$$

Ma $\mathrm{O}(3,\mathbb{C})$ è composto da due componenti, di determinanti ± 1, mentre $\mathrm{SL}(2,\mathbb{C})$ è connesso; quindi l'immagine di ρ è contenuta in $\mathrm{SO}(3,\mathbb{C})$.

Ora, $\mathrm{SL}(2,\mathbb{C})$ ha dimensione 3, così come $\mathrm{SO}(3,\mathbb{C})$: per questioni di dimensione si deduce che ρ è un rivestimento, con due fogli (perché $\ker(\rho) = \{\pm \mathrm{Id}\}$, sono le matrici che commutano con tutti i $\varphi(v)$): in conclusione, $\pi_1(\mathrm{SO}(3,\mathbb{C})) = \mathbb{Z}_2$.

Esempio 4.2.15. Si considera il caso generale, $\mathrm{SO}(n,\mathbb{C})$. Si può proiettare in $H \coloneqq \{ v \mid \langle v,v \rangle = 1 \}$ con la mappa $A \to Ae_1$. La fibra di questa mappa è data dalle matrici con la prima colonna fissata (ad esempio e_1 per la fibra sopra e_1), quindi anche la prima riga deve essere e_1; quello che rimane da fissare è una matrice $\tilde{A} \in \mathrm{SO}(n-1,\mathbb{C})$. Si ricava la fibrazione

$$\mathrm{SO}(n-1,\mathbb{C}) \to \mathrm{SO}(n,\mathbb{C}) \to H.$$

Per capire l'omotopia di $\mathrm{SO}(n,\mathbb{C})$ si deve studiare H: è fatto dai vettori complessi $x + iy$ tali che $\langle x,x \rangle - \langle y,y \rangle = 1$ e $\langle x,y \rangle = 0$. A sua volta, H può essere mandato su $\mathrm{T}\,S^{n-1}$, associando a (x,y) il vettore $({}^{x}/_{\|x\|}, y)$, dato che ${}^{x}/_{\|x\|} \in S^{n-1}$ e y è ortogonale a x. In realtà questa è una corrispondenza biunivoca, quindi $H \approx \mathrm{T}\,S^{n-1} \simeq S^{n-1}$. Procedendo come per $n = 3$, si ha che $\pi_1(\mathrm{SO}(n,\mathbb{C})) = \mathbb{Z}_2$ per $n \geq 3$.

Esempio 4.2.16. Si studia ora $\mathrm{SL}(n,\mathbb{C})$, proiettandolo su $\mathbb{C}^n \setminus \{0\}$: questa è un'azione di gruppo transitiva che dà una fibrazione, di fibra data dalle matrici che hanno come prima colonna (ad esempio) e_1, sulla prima riga hanno qualsiasi

	$\mathfrak{g}$	G	$\pi_1(G)$	$\mathrm{Z}(G)$
A_n	$\mathfrak{sl}(n+1,\mathbb{C})$	$\mathrm{SL}(n+1,\mathbb{C})$	$\{e\}$	$\mathbb{Z}_{n+1}$
B_n	$\mathfrak{so}(2n+1,\mathbb{C})$	$\mathrm{SO}(2n+1,\mathbb{C})$	$\mathbb{Z}_2$	$\{\mathrm{Id}\}$
		$\mathrm{Spin}(2n+1,\mathbb{C})$	$\{e\}$	$\{\mathrm{Id}\}$
C_n	$\mathfrak{sp}(2n,\mathbb{C})$	$\mathrm{Sp}(2n,\mathbb{C})$	$\{e\}$	$\mathbb{Z}_2$
D_n	$\mathfrak{so}(2n,\mathbb{C})$	$\mathrm{SO}(2n,\mathbb{C})$	$\mathbb{Z}_2$	$\mathbb{Z}_2$
		$\mathrm{Spin}(4m,\mathbb{C})$	$\{e\}$	$\mathbb{Z}_2\times\mathbb{Z}_2$
		$\mathrm{Spin}(4m+2,\mathbb{C})$	$\{e\}$	$\mathbb{Z}_4$

Tabella 1: Gruppi di Lie con algebre con certi diagrammi di Dynkin.

entrata e il resto è $\tilde{A}\in\mathrm{SL}(n-1,\mathbb{C})$, quindi la fibra è $\mathrm{SL}(n-1,\mathbb{C})\times\mathbb{C}^{n-1}$ che ha la stessa omotopia di $\mathrm{SL}(n-1,\mathbb{C})$. D'altra parte, $\mathbb{C}^n\setminus\{0\}$ si contrae su S^{2n-1}, che è semplicemente connesso per $n>1$, quindi $\pi_1(\mathrm{SL}(n,\mathbb{C}))=\{1\}$ per ogni $n>1$; per $n=1$, $\mathrm{SL}(n,\mathbb{C})\simeq\mathbb{C}^\star$, da cui $\pi_1(\mathrm{SL}(1,\mathbb{C}))=\mathbb{Z}$.

Esempio 4.2.17. Per $\mathrm{Sp}(2n,\mathbb{C})\coloneqq\{\,A\in\mathscr{M}_{2n}(\mathbb{C})\mid A^tMA=M\,\}$ con $M\coloneqq\left(\begin{smallmatrix}0 & I_n\\ -I_n & 0\end{smallmatrix}\right)$, si considera l'azione di $\mathrm{Sp}(2n,\mathbb{C})$ sull'insieme dei piani simplettici $H=\{\,(v,w)\mid v^tMw=1\,\}$ data da $A\mapsto(Ae_1,Af_1)$, dove $(e_1,\dots,e_n,f_1,\dots,f_n)$ è una base di $\mathbb{C}^{2n}$. Ancora, questa è un'azione transitiva, quindi si ha un fibrato, di fibra costituita da quattro blocchi matriciali A, B, C, D con $\left(\begin{smallmatrix}A & B\\ C & D\end{smallmatrix}\right)\in\mathrm{Sp}(2(n-1),\mathbb{C})$. Rimane da capire chi è H: può essere mandato in $\mathbb{C}^n\setminus\{0\}\simeq S^{2n-1}$ tramite la proiezione sulla prima coordinata; la fibra di questa azione è $\mathbb{C}^{n-1}$, retrattile. Quindi $\pi_1(\mathrm{Sp}(2n,\mathbb{C}))=\pi_1(\mathrm{Sp}(2(n-1),\mathbb{C}))$ e rimane da verificare chi è $\pi_1(\mathrm{Sp}(2,\mathbb{C}))$: la condizione di essere simplettica, in dimensione 2 è equivalente a $\det(A)=1$: $\mathrm{Sp}(2,\mathbb{C})=\mathrm{SL}(2,\mathbb{C})$, semplicemente connesso.

Dagli esempi visti, si deduce la tabella 1, che riassume i gruppi che hanno come algebre A_n, B_n, C_n, D_n e i loro rivestimenti universali. Il gruppo $\mathrm{Spin}(n,\mathbb{C})$ è un rivestimento doppio di $\mathrm{SO}(n,\mathbb{C})$.

4.3 Algebre di Clifford

31.05.2007

Sia V uno spazio vettoriale su K, q una forma quadratica qualsiasi su V; si definisce $\mathscr{T}(V)\coloneqq\bigoplus_{r\geq 0}V^{\otimes r}$; sia $\mathscr{I}_q(V)\coloneqq\langle v\otimes v+q(v)1\rangle$.

Definizione 4.3.1. L'*algebra di Clifford* di V rispetto a q è $\mathrm{Cl}(V,q)\coloneqq{}^{\mathscr{T}(V)}\!/\!{}_{\mathscr{I}_q(V)}$.

Si osserva che $v\otimes w+w\otimes v+2q(v,w)\in\mathscr{I}_q(V)$. Si considera $T_r\coloneqq\bigoplus_{i=0}^r V^{\otimes i}\subseteq\mathscr{T}(V)$. Sia π la proiezione di $\mathscr{T}(V)$ su $\mathrm{Cl}(V,q)$, allora si definiscono $\mathscr{F}_r\coloneqq\pi(T_r)$ e $\mathscr{G}^r\cong{}^{\mathscr{F}_r}\!/\!{}_{\mathscr{F}_{r-1}}$. Allora $\mathrm{Cl}(V,q)=\bigoplus_{r\geq 0}\mathscr{G}^r$.

Se $q=0$, si ha chiaramente $\mathrm{Cl}(V,q)=\Lambda V$, l'algebra esterna di V. Su di questa si pone la filtrazione data dai $\Lambda_r V$, contenenti gli elementi di ΛV fino al grado r.

Proposizione 4.3.2. *Si ha un isomorfismo canonico di spazi vettoriali filtrati* $\mathrm{Cl}(V,q)\cong\Lambda V$ *mediante le filtrazioni* $\mathscr{F}_r$ *su* $\mathrm{Cl}(V,q)$ *e* $\Lambda_r V$ *su* ΛV.

Dimostrazione. Si costruirà una mappa da ΛV a $\bigoplus_{r\geq 0}\mathscr{G}^r$; perché rispetti la filtrazione si devono costruire delle mappe $\Lambda^r V\to\mathscr{G}^r$. Innanzitutto si definisce la mappa $\pi\colon V^{\otimes r} \to \mathscr{G}^r$, con

$$\pi(v_1 \otimes \cdots \otimes v_r) = \frac{1}{n!} \sum_{\sigma \in \Sigma} \operatorname{sgn}(\sigma) v_{\sigma_1} \cdots v_{\sigma_r}$$

(se il campo non ha caratteristica 0, non si divide per il fattoriale). Questa mappa passa all'algebra esterna, cioè si annulla sugli elementi del tipo $\sum a_i \otimes v_i \otimes v_i \otimes b_i$, dove a_i e b_i sono prodotti tensoriali qualsiasi. Infatti, dentro $\mathscr{F}_r$, $v_i \otimes v_i$ è una costante, perciò $a_i \otimes v_i \otimes v_i \otimes b_i \in \mathscr{F}_{r-2}$, ma $\mathscr{F}_{r-2}$ è nullo in $\mathscr{G}^r$.

A questo punto, si ha una mappa $\pi\colon \Lambda^r V \to \mathscr{G}^r$. È una mappa suriettiva perché in $\mathrm{Cl}(V, q)$ si possono riordinare i termini, ma anche iniettiva: se $\varphi \mapsto 0$, si deve dimostrare che $\varphi \in \langle V \otimes V \rangle$; ma φ per andare in 0 deve essere fatto da una somma di elementi del tipo $a_i \otimes (v_i \otimes v_i + q(v_i)) \otimes b_i$ con $\deg a_i + \deg b_i = r - 2$, più una somma di elementi di grado minore di r; però $\varphi \in V^{\otimes r}$, la parte con $q(v_i)$ deve compensare la parte di grado più basso, cioè φ è somme di elementi del tipo $a_i \otimes v_i \otimes v_i \otimes b_i \in \langle V \otimes V \rangle$. $\square$

Da questo isomorfismo si ha che se $\dim V = n$, allora $\dim \mathrm{Cl}(V, q) = 2^n$. Se $(e_1, \ldots, e_n)$ è una base di V, i prodotti del tipo $e_{i_1} \cdots e_{i_r}$ con $i_1 < \cdots < i_r$, sono una base dell'algebra di Clifford. In particolare, $V \hookrightarrow \mathrm{Cl}(V, q)$ è un'applicazione iniettiva, il che ci permette di enunciare la seguente.

Proposizione 4.3.3. *Siano A un'algebra su un campo K, $f\colon V \to A$ lineare tale che $f(v)f(v) = -q(v)1$; allora esiste una unica $\tilde{f}\colon \mathrm{Cl}(V, q) \to A$ che solleva f. Inoltre, l'algebra di Clifford è l'unica algebra con questa proprietà.*

Dimostrazione. La mappa f si solleva a $f\colon \mathscr{T}(V) \to A$ in modo unico per la proprietà universale dell'algebra tensoriale; per l'ipotesi, f è nulla su $\mathscr{I}_q(V)$, quindi passa al quoziente a $\tilde{f}\colon \mathrm{Cl}(V, q) \to A$.

Si suppone ora di avere un'algebra C con questa proprietà; allora deve essere $V \hookrightarrow C$, quindi si ha una mappa $\mathrm{Cl}(V, q) \to C$, ma $V \hookrightarrow \mathrm{Cl}(V, q)$, quindi si ha anche una mappa $C \to \mathrm{Cl}(V, q)$. Componendo, si ha una unica mappa che, per quanto dimostrato, deve essere l'identità. $\square$

Osservazione 4.3.4. Sia $f\colon (V, q) \to (V', q')$ che rispetta la forma quadratica; allora f induce $\tilde{f}\colon \mathrm{Cl}(V, q) \to \mathrm{Cl}(V', q')$. Se si ha anche $g\colon (V', q') \to (V'', q'')$, allora $\tilde{g} \circ \tilde{f} = \widetilde{g \circ f}$. In particolare si ha una mappa $\mathrm{O}(V, q) \to \mathrm{End}(\mathrm{Cl}(V, q))$ e si dimostrerà che l'immagine in realtà va in $\mathrm{Aut}(\mathrm{Cl}(V, q))$.

La mappa $\alpha\colon V \to V\colon v \mapsto -v$, si solleva a $\alpha\colon \mathrm{Cl}(V, q) \to \mathrm{Cl}(V, q)$ con $\alpha^2 = \mathrm{Id}$. Allora si può scrivere $\mathrm{Cl}(V, q) = \mathrm{Cl}^0(V, q) \oplus \mathrm{Cl}^1(V, q)$, dove il primo è l'autospazio relativo all'autovalore 1 e il secondo è quello relativo a -1. Considerando gli indici modulo 2, si ha che $\mathrm{Cl}^i(V, q)\,\mathrm{Cl}^j(V, q) \subseteq \mathrm{Cl}^{i+j}(V, q)$: si ha una $\mathbb{Z}_2$-graduazione di $\mathrm{Cl}(V, q)$. Il grado di x corrisponde alla parità del numero di elementi che si devono moltiplicare per ottenere x.

Definizione 4.3.5. Siano A e B due algebre $\mathbb{Z}_2$-graduate. Si definisce il *prodotto tensoriale twistato* di A e B come $A \hat{\otimes} B$ dato, come spazio vettoriale, da $(A \hat{\otimes} B)^0 \coloneqq A^0 \otimes B^0 \oplus A^1 \otimes B^1$ e $(A \hat{\otimes} B)^1 \coloneqq A^0 \otimes B^1 \oplus A^1 \otimes B^0$; la struttura di algebra è data da $(a \otimes b)(c \otimes d) \coloneqq (-1)^{\deg b \deg c} ac \otimes bd$.

Proposizione 4.3.6. *Sia* $\mathrm{Cl}(V,q)$ *un'algebra di Clifford e sia* $(V,q) = (V_1,q_1) \oplus (V_2,q_2)$ *una decomposizione ortogonale di* (V,q)*, allora* $\mathrm{Cl}(V,q) = \mathrm{Cl}(V_1,q_1) \hat{\otimes} \mathrm{Cl}(V_2,q_2)$*.*

Dimostrazione. Se $v \in V$, $v = v_1 + v_2$ e si può mandare in $v_1 \otimes 1 + 1 \otimes v_2 \in \mathrm{Cl}(V_1,q_1) \hat{\otimes} \mathrm{Cl}(V_2,q_2)$. Sia f questa mappa; si deve verificare che $f(v)f(v) = -q(v)$, ma

$$\begin{aligned} f(v)f(v) &= (v_1 \otimes 1 + 1 \otimes v_2)(v_1 \otimes 1 + 1 \otimes v_2) = v_1^2 \otimes 1 + 1 \otimes v_2^2 = \\ &= -q_1(v_1) - q_2(v_2) = -q(v). \end{aligned}$$

La suriettività è data dal fatto che i vettori del tipo $v_1 \otimes 1$ generano $\mathrm{Cl}(V_1,q_1)$ e quelli del tipo $1 \otimes v_2$ generano $\mathrm{Cl}(V_2,q_2)$. L'iniettività si ottiene confrontando le dimensioni. □

Definizione 4.3.7. L'*applicazione trasposta* di $\mathrm{Cl}(V,q)$ è $\bullet^t \colon \mathrm{Cl}(V,q) \to \mathrm{Cl}(V,q) \colon v_1 \cdots v_r \mapsto v_r \cdots v_1$.

Definizione 4.3.8. Si definisce $\mathrm{Cl}^\star(V,q) \subseteq \mathrm{Cl}(V,q)$, l'insieme degli elementi invertibili di $\mathrm{Cl}(V,q)$.

Si dimostra che se $K \in \{\mathbb{R}, \mathbb{C}\}$, $\mathrm{Cl}^\star(V,q)$ è un gruppo di Lie e la sua algebra di Lie è $\mathfrak{cl}^\star(V,q) \coloneqq \mathrm{Cl}(V,q)$, con il prodotto bracket dato da $[x,y] \coloneqq xy - yx$.

Definizione 4.3.9. Si definisce l'*applicazione aggiunta* come $\mathrm{Ad} \colon \mathrm{Cl}^\star(V,q) \to \mathrm{Aut}(\mathrm{Cl}(V,q))$, ponendo $\mathrm{Ad}_\varphi(y) \coloneqq \varphi y \varphi^{-1}$.

Si definisce $\mathrm{ad} \colon \mathfrak{cl}^\star(V,q) \to \mathrm{Der}(\mathrm{Cl}(V,q))$ come $\mathrm{ad}_x(y) \coloneqq [x,y]$; ad è il differenziale dell'applicazione aggiunta.

D'ora in poi si supporrà che la caratteristica del campo sia diversa da 2.

Proposizione 4.3.10. *Sia* $v \in V$, $q(v) \neq 0$*. Allora* $\mathrm{Ad}_v(V) = V$*. Inoltre,* $-\mathrm{Ad}_v(w) = w - {}^{q(w,v)}/_{q(v,v)} v$*.*

Dimostrazione. Innanzitutto si deve dimostrare che $v \in \mathrm{Cl}^\star(V,q)$, ma questo è ovvio dato che si può scrivere $v^{-1} = -{}^{v}/_{q(v)}$. Ora, si ha

$$\begin{aligned} -q(v)\,\mathrm{Ad}_v(w) &= -q(v) v w v^{-1} = -q(v) v w \frac{v}{-q(v)} = v w v = \\ &= -v v w - 2q(v,w) v = q(v) w - 2q(v,w) v. \end{aligned}$$

Se si divide per $q(v)$, si ottiene il risultato. □

Definizione 4.3.11. Si definisce $P(V,q) \coloneqq \langle\, v \mid q(v) \neq 0 \,\rangle \subseteq \mathrm{Cl}^\star(V,q)$.

Osservazione 4.3.12. Il sottogruppo $P(V,q)$ si mappa tramite l'aggiunta Ad in $\mathrm{O}(V,q)$, dato che per la proposizione 4.3.10 se $q(v) \neq 0$, Ad_v conserva la forma quadratica.

Definizione 4.3.13. Dentro $P(V,q)$, si definiscono

$$\begin{aligned} \mathrm{Pin}(V,q) &\coloneqq \langle\, v \in V \mid q(v) = \pm 1 \,\rangle, \\ \mathrm{Spin}(V,q) &\coloneqq \mathrm{Pin}(V,q) \cap \mathrm{Cl}^0(V,q). \end{aligned}$$

Già si sa che $\mathrm{Pin}(V,q)$ viene mappato nel gruppo ortogonale. Si vuole dimostrare che $\mathrm{Spin}(V,q)$ riveste il gruppo speciale ortogonale.

Definizione 4.3.14. Si definisce l'*aggiunta twistata* come la mappa

$$\begin{array}{rrcl} \tilde{\mathrm{Ad}}\colon & \mathrm{Cl}^\star(V,q) & \to & \mathrm{GL}(\mathrm{Cl}(V,q)) \\ & \varphi & \mapsto & \big(\psi \mapsto \alpha(\varphi)\psi\varphi^{-1}\big)\,. \end{array}$$

Questa definizione è motivata dal fatto che, al contrario che per l'aggiunta, l'aggiunta twistata di un vettore v rispetto a w è proprio la riflessione.

Definizione 4.3.15. Si definisce $\tilde{P}(V,q) \coloneqq \Big\{ \varphi \in \mathrm{Cl}^\star(V,q) \mid \tilde{\mathrm{Ad}}_\varphi(V) = V \Big\}$.

Sicuramente, $P(V,q) \subseteq \tilde{P}(V,q)$. D'ora in poi si richiede che V sia di dimensione finita e q sia non degenere.

Proposizione 4.3.16. *Il nucleo di* $\tilde{\mathrm{Ad}}\colon \tilde{P}(V,q) \to \mathrm{GL}(V)$ *è* $K^\star$*.*

Dimostrazione. Sia $v_1, \dots, v_n$ una base ortogonale di V. In particolare, $v_iv_j = -v_jv_i$ per ogni $i \neq j$. Se $\varphi = \varphi_0 + \varphi_1$ appartiene al nucleo, allora $\tilde{\mathrm{Ad}}_\varphi(v) = v$ per ogni v, cioè $\alpha(\varphi)v\varphi^{-1} = v$ e $\alpha(\varphi)v = v\varphi$. Considerando lo spezzamento di φ, si ottiene $\varphi_o v = v\varphi_0$ e $\varphi_1 v = -v\varphi_1$.

Ora, si può scrivere $\varphi_0 = a_0 + v_1a_1$, dove a_0 e a_1 sono polinomi senza v_1, poiché $vv = -q(v)$. Allora $a_0v + v_1a_1v = va_0 + vv_1a_1$, che per $v = v_1$, dà $a_0v_1 + v_1a_1v_1 = v_1a_1 + v_1v_1a_1$ e usando le regole di scambio e il fatto che $v_1^2 = -q(v_1) \neq 0$, si ottiene che $a_1 = -a_1 = 0$, cioè $\varphi_0 = a_0$. Per induzione, si può dimostrare che φ_0 non contiene nessuno dei vettori, perciò deve essere un elemento del campo.

Per φ_1 si fa lo stesso ragionamento: si scrive $\varphi_1 = a_1 + v_1a_0$; applicando le stesse relazioni, si trova $a_0 = 0$, cioè $\varphi_1 \in K$. Ma φ_1 era di grado dispari, il che è assurdo a meno che φ_1 non sia nullo. Allora $\varphi = \varphi_0 + \varphi_1 = \varphi_0 \in K^\star$. □

Definizione 4.3.17. Sia $\varphi \in \mathrm{Cl}(V,q)$; si definisce la *norma* di φ come $\mathrm{N}(\varphi) \coloneqq \varphi\alpha(\varphi^t)$.

Ovviamente, se $v \in V$, $\mathrm{N}(v) = q(v)$.

Proposizione 4.3.18. *Si ha* $\mathrm{N}\colon \tilde{P}(V,q) \to K^\star$*; inoltre questa applicazione è un morfismo.*

Dimostrazione. Se $\varphi \in \tilde{P}(V,q)$, allora $\alpha(\varphi)v\varphi^{-1} \in V$; essendo un vettore,

$$\alpha(\varphi)v\varphi^{-1} = \left(\alpha(\varphi)v\varphi^{-1}\right)^t = \left(\varphi^{-1}\right)^t v\alpha(\varphi^t).$$

Moltiplicando per φ^t e $\alpha(\varphi^t)^{-1}$, si ha

$$v = \varphi^t\alpha(\varphi)v\varphi^{-1}\alpha(\varphi^t)^{-1} = \alpha(\alpha(\varphi^t)\varphi)v(\alpha(\varphi^t)\varphi)^{-1} = \tilde{\mathrm{Ad}}_{\alpha(\varphi^t)\varphi}(v),$$

cioè $\alpha(\varphi^t)\varphi \in \ker(\tilde{\mathrm{Ad}}) = K^\star$; ma $\alpha(\varphi^t)\varphi$ è anche uguale a $\alpha\,\mathrm{N}(\varphi^t)$. Ora, α manda $\tilde{P}(V,q)$ in se stesso, da cui $\mathrm{N}(\varphi^t) \in K^\star$. Ma anche $\bullet^t$ manda $\tilde{P}(V,q)$ in se stesso, quindi $\mathrm{N}(\varphi) \in K^\star$.

È anche morfismo:

$$\begin{aligned} \mathrm{N}(\varphi\psi) &= \varphi\psi\alpha(\psi^t\varphi^t) = \varphi\psi\alpha(\psi^t)\alpha(\varphi^t) = \varphi\,\mathrm{N}(\psi)\alpha(\varphi^t) = \\ &= \mathrm{N}(\psi)\varphi\alpha(\varphi^t) = \mathrm{N}(\psi)\,\mathrm{N}(\varphi), \end{aligned}$$

da $\mathrm{N}(\psi) \in K^\star$. □

Proposizione 4.3.19. *L'aggiunta twistata è un morfismo da $\tilde{P}(V,q)$ in $\mathrm{O}(V,q)$.*

Dimostrazione. Si ha $\mathrm{N}(\alpha\varphi) = \alpha(\varphi)\varphi^t = \alpha(\varphi\alpha(\varphi^t)) = \alpha(\mathrm{N}(\varphi)) = \mathrm{N}(\varphi)$. Si vuole dimostrare che $q(\tilde{\mathrm{Ad}}_\varphi(v)) = q(v)$. Se si prende lo spazio $V^\star$ dei v per cui $q(v) \neq 0$, basta mostrare la proprietà per questo spazio. Infatti, $\mathrm{N}(\tilde{\mathrm{Ad}}_\varphi(v)) = \mathrm{N}(\alpha(\varphi)v\varphi^{-1}) = \mathrm{N}(\alpha(\varphi))\,\mathrm{N}(v)\mathrm{N}(\varphi)^{-1} = \mathrm{N}(v) = q(v)$. D'altra parte, $\mathrm{N}(\tilde{\mathrm{Ad}}_\varphi(v)) = q(\tilde{\mathrm{Ad}}_\varphi(v))$ perché $\tilde{\mathrm{Ad}}_\varphi(v) \in V$. □

Si era visto che $\tilde{\mathrm{Ad}}$ associava a $v \in P(V,q) \subseteq \tilde{P}(V,q)$ la riflessione $\rho_v \in \mathrm{O}(V,q)$. Ma questo implica la surettività, poiché le trasformazioni ortogonali sono generate dalle riflessioni (teorema di Cartan-Dieudonné).

Corollario 4.3.20. *L'applicazione* $\tilde{\mathrm{Ad}}\colon P(V,q) \to \mathrm{O}(V,q)$ *è suriettiva.*

Definizione 4.3.21. Un campo K è detto *campo spin* se per ogni elemento $\lambda \in K$, almeno una tra $\lambda = t^2$ e $\lambda = -t^2$ ha soluzione.

Poiché quando si fa la riflessione rispetto a un vettore v non importa la sua norma, si possono rinormalizzare tutti i vettori di un prodotto in modo da avere $q(v) = \pm 1$; questo però richiede di saper risolvere equazioni del tipo $t^2 = \pm a$, dato che $q(\lambda v) = \lambda^2 v$.

Teorema 4.3.22. *Se K è un campo spin e V è uno spazio vettoriale su K, allora si hanno le successioni esatte*

$$
\begin{gathered}
0 \to F \to \mathrm{Pin}(V,q) \to \mathrm{O}(V,q) \to 0 \\
0 \to F \to \mathrm{Spin}(V,q) \to \mathrm{SO}(V,q) \to 0,
\end{gathered}
$$

con $F = \{\pm 1\} = \mathbb{Z}_2$ se $\sqrt{-1} \notin K$; $F = \{\pm 1, \pm i\} = \mathbb{Z}_4$ se $\sqrt{-1} \in K$.

Riferimenti bibliografici

[Ada83] Adams, John F.: *Lectures on Lie groups*. University of Chicago Press, 1983.

[Hum94] Humphreys, James E.: *Introduction to Lie algebras and representation theory*. Graduate Texts in Mathematics. Springer-Verlag, 1994.

[LM90] Lawson, Herbert B. e Marie Louise Michelsohn: *Spin geometry*. Princeton University Press, 1990.

[Pro06] Procesi, Claudio: *Lie groups: an approach through invariants and representations*. Springer-Verlag, 2006.

[Var84] Varadarajan, Veeravalli S.: *Lie groups, Lie algebras, and their representations*. Graduate Texts in Mathematics. Springer-Verlag, 1984.